



HOSPITAL DAS CLÍNICAS DA UNIVERSIDADE FEDERAL DE MINAS GERAIS

Avenida Professor Alfredo Balena, nº 110 - Bairro Santa Efigênia

Belo Horizonte-MG, CEP 30130-100

- <http://hc-ufmg.ebserh.gov.br>

Termo de Referência - TI - SEI

TERMO DE REFERÊNCIA

1. INTRODUÇÃO

1.1. O Hospital das Clínicas da UFMG/Ebserh, hospital universitário, público e geral, integrado 100% ao Sistema Único de Saúde (SUS), atua no atendimento à sociedade, na formação de recursos humanos, no desenvolvimento de pesquisas e na produção e incorporação de tecnologia na área da saúde por meio de atividades de ensino, pesquisa, extensão e assistência.

1.2. Atende todas as especialidades e subespecialidades oferecidas pelo SUS com exceção da radioterapia, constituindo-se como referência em alta complexidade para todo o estado de Minas Gerais.

1.3. O HC-UFMG/Ebserh realiza, em média, 30 mil consultas ambulatoriais por mês, 2.100 consultas de emergência, 4.500 cirurgias ambulatoriais e 160 mil exames ambulatoriais.

1.4. O Hospital integra a Rede Ebserh desde dezembro de 2013, estatal vinculada ao Ministério da Educação (MEC) que foi criada em 2011 e, atualmente, administra 40 hospitais universitários federais, apoiando e impulsionando suas atividades por meio de uma gestão de excelência.

1.5. A Empresa Brasileira de Serviços Hospitalares (Ebserh) é uma empresa pública de direito privado, criada pela Lei Federal nº 12.550, de 15 de dezembro de 2011 com Estatuto Social aprovado na Assembleia Geral Extraordinária realizada no dia 10 de novembro de 2020.

1.6. A Ebserh tem por finalidade a prestação de serviços gratuitos de assistência médico-hospitalar, ambulatorial e de apoio diagnóstico e terapêutico à comunidade, assim como a prestação às instituições públicas federais de ensino ou instituições congêneres de serviços de apoio ao ensino, à pesquisa e à extensão, ao ensino-aprendizagem e à formação de pessoas no campo da saúde pública, observada, nos termos do art. 207 da Constituição Federal, a autonomia universitária.

1.7. As atividades de prestação de serviços de assistência à saúde estão inseridas integral e exclusivamente no âmbito do Sistema Único de Saúde (SUS). No desenvolvimento de suas atividades de assistência à saúde, a Ebserh observará as diretrizes e políticas estabelecidas pelo Ministério da Saúde.

1.8. A Ebserh tem como missão aprimorar a gestão dos Hospitais Universitários Federais - HUFs e congêneres, prestar atenção à saúde de excelência e fornecer um cenário de prática adequado ao ensino e pesquisa para docentes e discentes.

2. OBJETO DA CONTRATAÇÃO (IN SGD/ME Nº 94/2022 - ART. 13)

Registro de Preços para Aquisição de equipamentos Firewall com recursos de próxima geração (NGFW), com Subscrição das Licenças de Segurança, suporte técnico e garantia por 60 meses, incluindo Serviço de Instalação e configuração.

3. DESCRIÇÃO DA SOLUÇÃO DE TIC (IN SGD/ME Nº 94/2022 - ART. 14)

3.1. **Registro de preços para Aquisição de equipamentos Firewall com recursos de próxima geração (NGFW), com Subscrição das Licenças de Segurança, suporte técnico e garantia por 60 meses, incluindo Serviço de Instalação e configuração**, para atendimento à demanda do Hospital das Clínicas da Universidade Federal de Minas Gerais - HC-UFMG administrado pela Empresa Brasileira de Serviços Hospitalares - Ebserh.

3.2. A solução de proteção de rede aqui proposta é composta pelo provisionamento de 02 (duas) appliances de firewall com recursos de segurança tidos como de próxima geração (NGFW) totalmente integrados, tais como: filtro de conteúdo, filtro de dados, controle granular de aplicações, inclusive da camada 7 do modelo OSI/ISO, sistema de prevenção de instrução (IPS), anti-vírus, anti-spyware, proteção contra ameaças avançadas e malwares, inclusive zero-day, VPN IPsec e VPN SSL, qualidade de serviço e

modelagem de tráfego (QoS), incluindo suporte e garantia por 60 (sessenta) meses, bem como instalação e configuração de toda a solução de proteção de rede;

3.3. **O critério de julgamento adotado será o de menor preço do item**, observadas as exigências contidas nesse Termo de Referência, no Edital e seus **Anexos** quanto às especificações do objeto.

3.4. Bens e serviços que compõem a solução

ID.	DESCRIÇÃO DO BEM OU SERVIÇO	CÓDIGO CATMAT	QUANTIDADE	UNIDADE
1	Equipamento firewall com recursos de próxima geração (NGFW), com Subscrição das Licenças de Segurança, suporte técnico e garantia por 60 meses, incluindo Serviço de Instalação e configuração.	481646	02	Unidade

4. JUSTIFICATIVA PARA A CONTRATAÇÃO (IN SGD/ME Nº 94/2022 - ART. 15)

4.1. MOTIVAÇÃO DA CONTRATAÇÃO

4.1.1. O Hospital das Clínicas da Universidade Federal de Minas Gerais (HC-UFMG), possui diversos processos de trabalho informatizados, entre eles, a tramitação de processos administrativos internos, através da ferramenta "Sistema Eletrônico de Informações (SEI)", a realização de registros médicos e assistenciais por meio do "Aplicativo de Gestão para Hospitais Universitários (AGHU)", atividades educacionais realizadas nas dependências da instituição, realização de videoconferências e reuniões diretamente relacionadas com o trabalho que é desenvolvido dentro da instituição. Outros processos também auxiliam na execução das tarefas dentro de diversas áreas, como o acesso à internet (rede cabeada e sem fio), acesso à intranet, solicitação de materiais, e suporte técnico através de sistema de chamados, tanto para manutenção e correção da infraestrutura de tecnologia de informação, quanto predial, serviço de telefonia, impressão, serviços de engenharia clínica, entre outros.

4.1.2. Os ganhos de eficiência e produtividade com a informatização de processos de trabalho estão diretamente relacionados com a capacidade da tecnologia de informação em garantir disponibilidade, confiabilidade, desempenho e integridade da infraestrutura tecnológica que provê estes serviços. Trata-se de um processo contínuo, onde novas ameaças e vulnerabilidades são descobertas, quase que diariamente. Uma das maneiras de se melhorar a segurança da informação, considerando os diferentes ambientes, corporativo e hospitalar, se dá através de mecanismos de proteção de rede de dados com recursos de próxima geração, entre eles, a identificação de aplicações em uso na rede de dados, a prevenção de ameaças, a identificação de usuários e controle de permissões. Estes mecanismos atuam com filtros eletrônicos que examinam todo o tráfego de rede, aplicando um conjunto de regras de segurança e analisando o envio e recebimento de informações, estabelecendo o que pode ser executado. Com este tipo de implementação pode-se monitorar e analisar todo o tráfego de rede, garantindo maior segurança às informações institucionais

4.1.3. Constata-se que quanto maior e mais diversificado for o escopo de ativos de rede, mais difícil e complexo tende a ser sua administração, consequentemente atividades como mitigação de vulnerabilidades, aplicação de atualizações de segurança, correções e melhorias tornam-se mais necessárias e dispendiosas, por outro lado, maiores e mais diversificadas são as possibilidades de ataques, falhas, ameaças e explorações de vulnerabilidades.

4.1.4. O Hospital das Clínicas da Universidade Federal de Minas Gerais (HC-UFMG) implanta e gerencia serviços e recursos de tecnologia da informação e comunicação por meio do Setor de Tecnologia da Informação e Saúde Digital (SETISD). Saliencia-se a crescente demanda por recursos e serviços computacionais, competindo com a gerência dos recursos já existentes, através de melhorias e correções, além das atividades de gestão e fiscalização de vários contratos de TIC. Ressalta-se a diversa gama de atividades executadas pelo SETISD frente ao limitado conjunto de recursos humanos lotados no setor, o que faz com que as atividades do escopo de segurança da informação, como aplicação de atualizações, nem sempre sejam possíveis de serem priorizadas adequadamente, pois competem com as demais atividades já listadas anteriormente. Além disso, se tem a necessidade constante do processo permanente de modernização do ambiente tecnológico.

4.1.5. Neste contexto de crescimento tecnológico, aumenta a preocupação com a segurança e proteção dos dados e aplicativos. Legislações como a Lei Geral de Proteção de Dados (LGPD) preveem punições às empresas que não aplicam as melhores práticas de gestão com relação à segurança dos dados de seus clientes. Além da preocupação com punições como multas, a LGPD prevê também que empresas ao serem exploradas, com extravio de informações de clientes, sejam obrigadas a dar visibilidade ao fato, exigindo a comunicação do ocorrido aos clientes que possuem dados resguardados por elas, sendo um imensurável dano à confiança na marca.

4.1.6. Pesquisas do Gartner apontam que $\frac{3}{4}$ dos ataques procuram explorar vulnerabilidades ao nível da aplicação. Essa abordagem significa que o hacker, ao descobrir uma brecha no aplicativo, pode explorar a situação para extração de dados de maneira lenta e de difícil detecção.

4.1.7. O Marco Civil da Internet (Lei nº 12.965/2014) e a recente Lei Geral de Proteção de Dados (Lei nº 13.709/2018), fez com que o SETISD criasse a necessidade para atender aos requisitos voltado a uma maior proteção dos dados pessoais e do tráfego de dados que atualmente já é realizado no ambiente do HC-UFMG.

4.1.8. A solução de proteção de rede proporcionará a otimização e atingimento dos objetivos de segurança da informação, mesmo quando os ativos de rede estiverem com vulnerabilidades ou suscetíveis a ameaças, ataques e falhas de segurança da informação.

4.2. OBJETIVOS DA CONTRATAÇÃO:

- a) Proteger os recursos de rede computacional, à qual se interliga o parque de servidores, para disponibilizar serviços de segurança, evitando e protegendo a rede contra ataques internos e externos;
- b) Preservar a integridade, confidencialidade e disponibilidade das informações guardadas em seus ambientes de atuação contra destruição, divulgação indevida e acessos não autorizados, acidentais ou intencionais, garantindo a continuidade dos serviços prestados.
- c) Aumentar a capacidade e o quantitativo de equipamentos de segurança da instituição de modo a eliminar o ponto único de falha existente no momento.

4.2.1. O equipamento aqui listado tem por objetivo garantir a manutenção dos serviços do Setor de Gestão de Tecnologia da Informação e Saúde Digital (SETISD). Este equipamento faz parte da solução de proteção de rede, que é composta por dois appliances de firewall com recursos de próxima geração, com Subscrição das Licenças de Segurança, suporte técnico e garantia por 60 meses, incluindo Serviço de Instalação e configuração, para prover alta disponibilidade e garantir o funcionamento contínuo da rede de dados da instituição;

4.3. Quanto à utilização da modalidade Registro de Preços, o objeto em questão se enquadra na hipótese II do art. 3º do Decreto nº. 11.462/23, visto que em se tratando de bens a serem adquiridos de forma parcelada, e não necessariamente de forma imediata, onde o fornecedor disponibiliza os bens a preços e prazos registrados em Ata específica e que, a aquisição é feita quando melhor convier à Administração e outras entidades que integram a Ata, é recomendada a adoção da modalidade de Sistema de Registro de Preços;

4.4. A natureza dos bens a serem contratados é comum, nos termos do inciso XIII, art. 6º, da Lei 14.133, de 2021;

XIII - bens e serviços comuns: aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado;

4.5. ALINHAMENTO AOS INSTRUMENTOS DE PLANEJAMENTOS INSTITUCIONAIS

4.5.1. Esta aquisição está alinhada ao:

- I - Objetivo Estratégico, "OE18 - Promover Inovação e Transformação digital na Rede Ebserh", disponível no MAPA ESTRATÉGICO 2024-2028 disponível em <https://www.gov.br/ebserh/pt-br/governanca/gestao-estrategica/mapa-estrategico>;
- II - Objetivo Estratégico de Tecnologia da Informação e Comunicação do HC-UFMG, "OETIC06 - Melhorar a segurança das informações eletrônicas da instituição" disponível em [PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação](#), pág. 20;
- III - Necessidade "NE40 - Reduzir a vulnerabilidade de acesso à rede" disponível em [PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação](#), pág. 28.

IV - Acordo Organizativo de Compromissos (AOC), processo SEI (23477.017796/2023-33), Grupo "5. Reestruturação Física e Tecnológica", subgrupo "5.4 – TI (equipamento, software, serviço)";

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
ID	Documento	Objetivos Estratégicos
OE18	Mapa Estratégico da Ebserh	Promover Inovação e Transformação digital na Rede Ebserh
4.07	Plano Diretor Estratégico 2019-2023 - HC-UFGM	Criação de Estratégia Híbrida de Infraestrutura de TI
OETIC01	PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação HC-UFGM 2022 - 2024	Melhorar a experiência dos clientes no uso dos serviços de TIC
OETIC05	PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação HC-UFGM 2022 - 2024	Melhorar as condições de uso dos sistemas institucionais
OETIC06	PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação HC-UFGM 2022 - 2024	Melhorar a segurança das informações eletrônicas da instituição
OETIC09	PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação HC-UFGM 2022 - 2024	Prover o HC-UFGM de infraestrutura tecnológica adequada
OETIC20	PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação HC-UFGM 2022 - 2024	Garantir a continuidade dos serviços de TIC

ALINHAMENTO AO PDTIC 2022 - 2024			
ID	Ação do PDTIC	ID	Meta do PDTIC associada
A40	Adquirir firewall de borda	M40	Processo escrito, homologado e equipamento instalado

ALINHAMENTO AO ACORDO ORGANIZATIVO DE COMPROMISSOS (AOC)	
Item	Descrição
Grupo 05	Reestruturação Física e Tecnológica
Subgrupo 5.4	TI (equipamento, software, serviço)

4.6. ESTIMATIVA DA DEMANDA

4.6.1. Atualmente o Hospital das Clínicas da Universidade Federal de Minas Gerais (HC-UFGM) conta em sua infraestrutura de TI como ferramentas críticas para proteção da sua rede de dados com uma solução de Firewall de Próxima Geração, modelo PA-850 e software Panorama de gerenciamento a armazenamento de logs centralizado, ambos da fabricante Palo Alto Networks.

4.6.2. Por essa solução, appliance e Panorama, passa todo o tráfego da instituição, tornando-o portanto, extremamente crítico e também como ponto único de falha do ambiente de rede. Como solução para mitigar este risco, a estimativa é adquirir dois novos appliances do mesmo fabricante para permitir a implementação de um ambiente de alta disponibilidade e ainda ampliar as features de segurança.

4.6.3. A escolha por Firewalls de Próxima Geração do mesmo fabricante das soluções já em uso traz consigo vantagens consideráveis para o gerenciamento e visibilidade da rede do HC-UFGM, especialmente quando integrados ao software Panorama existente. O Panorama oferece uma plataforma centralizada para gerenciamento de políticas, monitoramento de tráfego e análise de logs, proporcionando uma visão unificada e simplificada de toda a infraestrutura de segurança do hospital.

4.6.4. A integração dos Firewalls de Próxima Geração da Palo Alto com o software Panorama existente permitirá estender essas capacidades de gerenciamento e visibilidade, garantindo uma administração mais eficiente e uma resposta mais ágil a possíveis ameaças. Além disso, a equipe técnica do hospital já está familiarizada com as operações das ferramentas existentes, o que permite que a adoção dos novos firewall seja perfeitamente integrada ao ambiente do HC-UFGM, minimizando o tempo de aprendizado, tornando a implantação dos novos equipamentos mais célere, com baixo impacto no ambiente e maximizando o retorno sobre o investimento realizado.

4.6.5. Ao considerar o contexto da segurança cibernética em constante evolução e a importância crítica da proteção dos ativos digitais do HC-UFGM, a aquisição dos Firewall de Próxima Geração de um mesmo fabricante representa um investimento estratégico para fortalecer a postura de segurança do hospital, aumentando sua capacidade de defesa contra ameaças cibernéticas, mas também contribuirá para a eficiência operacional e a proteção contínua dos dados confidenciais da instituição.

4.6.6. **Para a solução de proteção de rede aqui proposta, tem-se a seguinte composição:**

4.6.7. Registro de preço de 02 (duas) appliances de firewall com recursos de próxima geração, com garantia e suporte por no mínimo 60 meses, para prover alta disponibilidade e garantir o funcionamento contínuo da rede de dados da instituição;

4.6.8. Para calcular o quantitativo de unidades necessários, levou-se em consideração o mínimo necessário para promover um ambiente de alta disponibilidade, no caso, uma solução composta de dois equipamentos ativo-ativo.

4.6.9. Um serviço de instalação, configuração e treinamento nas dependências do HC-UFGM;

4.6.10. Tabela contendo as características e quantitativo dos itens:

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE
01	Appliance de firewall de próxima geração (NGFW) com suporte técnico e garantia de 60 meses, incluindo serviço de instalação e configuração.	Unidade	02

4.7. **PARCELAMENTO DA SOLUÇÃO DE TIC**

4.8. O objeto da pretendida contratação definido no item 04 deste Termo de Referência se configura como um único item de solução de Tecnologia da Informação, portanto, não se aplica neste contexto a possibilidade de parcelamento da solução de TIC.

4.9. **RESULTADOS E BENEFÍCIOS A SEREM ALCANÇADOS**

4.9.1. Melhorar a gestão e operação de regras de segurança;

4.9.2. Redução de vulnerabilidades da instituição;

4.9.3. Criação de políticas de proteção da rede contra ataques de agentes mal intencionados, além de melhor controle de utilização da rede, com a aplicação de filtros e bloqueios conforme o usuário e aplicações, controlando a utilização dos recursos e o acesso a sites indesejados para a instituição, além da geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, e usuários, auxiliando na tomada de decisões;

4.9.4. Melhor aproveitamento de tempo e desempenho da equipe de TIC da instituição hospitalar;

4.9.5. Maior aderência às legislações vigentes, principalmente à LGPD, ao Marco Civil da Internet lei 12.965/2014) e à Estratégia de Governo Digital (decreto 10.332/2020), bem como maior facilidade da aplicação de tais comandos legais;

4.9.6. Uso mais seguro dos serviços internos e externos da instituição, bem como a garantia da integridade, confiabilidade, disponibilidade e desempenho no uso dos recursos, e facilidade de TIC, bem

como no tratamento de dados e informações;

4.9.7. Reduzir os riscos de paralisação ou redução da continuidade de serviços assistenciais, administrativos e de ensino, bem como propiciar condições ideais de funcionamento do parque computacional existente no hospital, de forma a manter contínua, eficiente e com qualidade, os serviços públicos prestados aos usuários do Sistema Único de Saúde (SUS).

IN SGD/ME Nº 94/2022 - ART. 16 INCISO I

5. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO (IN SGD/ME Nº 94/2022 - ART. 16)

5.1. REQUISITOS DE NEGÓCIO (IN SGD/ME Nº 94/2022 - Art. 16, inciso I, alínea a)

5.1.1. As necessidades de negócio, também chamadas de requisitos do negócio, segundo o Corpo de Conhecimento de Análise de Negócios (Guia BABOK v. 2.0), são metas de mais alto nível, objetivos ou necessidades da organização. Descrevem as razões pelas quais um projeto foi iniciado, os objetivos que o projeto vai atingir e as métricas que serão utilizadas para medir o seu êxito. Nesse sentido, a presente seção visa descrever as necessidades de negócios que conduzirão as análises de soluções e definição da solução mais adequadas a tais objetivos organizacionais, conforme relação a seguir:

5.1.2. Este estudo visa garantir a viabilidade da aquisição de uma solução de firewall descritos pelo Documento de Oficialização da Demanda (35593943), tendo a missão em atender com qualidade às expectativas dos usuários em seus serviços, recorrendo aos recursos tecnológicos para desempenhar com plenitude suas atividades.

5.1.3. A sustentação tecnológica inclui-se a manutenção de TIC como condição prioritária para o contínuo serviço na organização de processos e métodos de trabalho na área da saúde. Nesta linha tecnológica foram desenvolvidas ações importantes suprimindo, especialmente, as necessidades dos setores essenciais como atendimentos ambulatoriais, controle de internações, controle de estoques diversos, farmácia, prescrição/evolução médica, nutrição, exames laboratoriais, diagnóstico por imagem, cirurgias, entre outros, havendo assim a necessidade de suprir as demandas existentes.

5.1.4. Para cumprir a sua missão e atender com qualidade às expectativas dos usuários dos seus serviços é indispensável que o HC-UFMG/Ebserh mantenha em perfeito funcionamento e promova melhorias contínuas em sua infraestrutura de TIC, fornecendo o suporte necessário à utilização dos recursos informacionais e dos sistemas aplicativos, orientando, avaliando e, eventualmente, corrigir suas estratégias e políticas, sempre que necessário, seja por exigência de nova legislação, seja através de novas tecnologias que possam exigir alteração na infraestrutura computacional.

5.1.5. Também deve-se considerar que o uso de tecnologias digitais tornou-se um meio cada vez mais presente na área da saúde e a transformação digital do setor abrange as ações de telemedicina, telessaúde, atividades inerentes às imagens e laudos dos pacientes através de solução PACS (armazenamento de imagens digitais), de áreas tradicionais da informática em saúde, como gestão hospitalar e prontuário eletrônico – uma esfera de intervenções tecnológicas denominada “Saúde Digital” pela Organização Mundial da Saúde (OMS).

5.1.6. Existe a necessidade de aquisição de uma solução de firewall para expandir os controles de segurança e permitir:

- a) Autenticação e rastreabilidade das informações de acesso dos usuários pelo período mínimo de 01 ano de acordo com o Marco Civil da Internet, Lei nº 12.965/2014;
- b) Preservação da integridade e da confidencialidade dos dados dos usuários, para conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018);
- c) Melhorar o nível de qualidade e segurança dos serviços das aplicações internas da instituição;
- d) Proteção da infraestrutura de TI desta instituição, de modo a impedir que a mesma seja utilizada para outros fins (por exemplo: link de internet utilizado para download de conteúdo ilícito/indevido, diferente das atividades fim realizadas pela instituição, ou ataques de negação de serviço distribuídos – DDoS, ou ainda uso de aplicações diferentes das homologadas pela instituição).
- e) Melhorar a proteção da rede interna por meio de regras de segurança dinâmicas atualizadas automaticamente pela solução de firewall.

- f) Permitir uma melhor gestão e controle de acesso aos sites externos, principalmente ao bloqueio de sites de alto riscos e de medias sociais.

5.2. REQUISITOS DE CAPACITAÇÃO (IN SGD/ME Nº 94/2022 - Art. 16, inciso I, alínea b)

- 5.2.1. Deverá possuir suporte técnico especializado e garantia do fabricante, durante a vigência do contrato, todos os produtos ofertados que compõem a solução de segurança, de modo que garanta a reposição de peças, atualizações de segurança, atualizações sistêmicas, correção de bugs e assistência técnica para casos de dúvidas, incidentes ou indisponibilidade da solução ofertada.
- 5.2.2. Deverá ser disponibilizado canais de atendimento, com acesso direto ao fabricante, para abertura de chamados técnicos sempre que necessário. Deverá ser fornecida toda documentação que apoie no diagnóstico e administração da solução ofertada.
- 5.2.3. Durante a vigência do contrato deverá ser prestado o serviço de suporte técnico que permita solicitar informações, reportar incidentes ou esclarecer dúvidas quanto à utilização dos produtos da solução ofertada.
- 5.2.4. Deverá garantir que o serviço de suporte técnico não comprometa a garantia da solução ofertada.
- 5.2.5. Deverá ser previsto acordo de nível serviço (SLA) para casos de acionamento do serviço de suporte técnico e garantia.
- 5.2.6. Deverá ser previsto solução de contorno em caso de acionamento da garantia que vise reduzir o tempo de indisponibilidade da solução ofertada

5.3. REQUISITOS LEGAIS (IN SGD/ME Nº 94/2022 - Art. 16, inciso I, alínea d)

- 5.3.1. Lei 13.303, de 30 de junho de 2016 - Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios;
- 5.3.2. Instrução Normativa da Secretaria de Governo Digital do Ministério da Economia, nº 94, de 23 de dezembro de 2022 - 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 - SISF do Poder Executivo Federal;
- 5.3.3. Regulamento de Licitações e Contratos da Ebserh - Regulamenta as licitações e contratos para aquisição de bens e serviços pela Ebserh, e dá outras providências, disponível em: <<https://www.gov.br/ebserh/pt-br/acesso-a-informacao/licitacoes-e-contratos/legislacao-e-normas-de-licitacoes-e-contratos>>;
- 5.3.4. Norma - SEI nº 2/2019/DAI-EBSERH - Norma Operacional dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens, contratação de serviços em geral, bem como alterações contratuais;
- 5.3.5. Portaria nº 20, de 14 de junho de 2016 - Dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional e dá outras providências;
- 5.3.6. Instrução Normativa da Secretaria de Governo Digital do Ministério da Economia, nº 5, de 30 de agosto de 2021 - Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.
- 5.3.7. Decreto-Lei nº 200, de 25 de fevereiro de 1967 - Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências;
- 5.3.8. Decreto nº 10.024, de 20 de setembro de 2019 - Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal;
- 5.3.9. Decreto nº 7.174/2010, de 12 de maio de 2010 - 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;
- 5.3.10. Lei nº 13.709, de 14 de agosto de 2018 - dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o

objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

5.3.11. Decreto nº 9.373, de 11 de maio de 2018 - Dispõe sobre a alienação, a cessão, a transferência, a destinação e a disposição final ambientalmente adequadas de bens móveis no âmbito da administração pública federal direta, autárquica e fundacional;

5.3.12. Instrução Normativa SLTI/MP nº 1 de 19 de janeiro de 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;

5.3.13. Decreto 7.746/12 de 5 de junho de 2012 - Regulamenta o art. 3º da Lei nº 8.666, de 21 de junho de 1993, para estabelecer critérios e práticas para a promoção do desenvolvimento nacional sustentável nas contratações realizadas pela administração pública federal direta, autárquica e fundacional e pelas empresas estatais dependentes, e institui a Comissão Interministerial de Sustentabilidade na Administração Pública – CISAP;

5.3.14. Lei nº 12.305, de 2 de agosto de 2010 - Institui a Política Nacional de Resíduos Sólidos; altera a Lei no 9.605, de 12 de fevereiro de 1998; e dá outras providências;

5.3.15. Decreto nº 10.779, de 25 de agosto de 2021 - Estabelece medidas para a redução do consumo de energia elétrica no âmbito da administração pública federal;

5.3.16. Resolução CGPAR Nº 29, de 05 de abril de 2022 - Estabelece orientações às empresas estatais federais para a contratação de bens e serviços de tecnologia da informação - TI.

5.4. **REQUISITOS DE MANUTENÇÃO** (IN SGD/ME Nº 94/2022 - Art. 16, inciso I, alínea d)

5.4.1. Entende-se como manutenção as atividades relativas ao bom funcionamento da solução que abrangem: garantia de funcionamento, suporte técnico e atualização da solução;

5.4.2. A contratada deverá prestar garantia de funcionamento, suporte técnico e atualização pelo período de 60 meses, contados da data do aceite definitivo da instalação, configuração e ativação da solução. É de responsabilidade da contratada garantir que o suporte padrão de 60 meses registrado junto ao fabricante abranja todo o período contratado, atendido no local da instituição (on-site), com atendimento durante 24 horas, nos sete dias da semana (24x7), abrangendo-se todo e qualquer defeito, desde seu projeto, fabricação e desempenho dos equipamentos e serviços de segurança inclusos na solução;

5.4.3. Em caso de defeitos de fabricação, o serviço de garantia incluirá o envio de peças ou equipamentos de reposição nos locais apontados no instrumento licitatório, no mínimo na modalidade NDB (Next Business Day);

5.4.4. O suporte técnico será acionado, no mínimo, por uma das opções abaixo:

- a) junto ao fabricante da solução de proteção de rede;
- b) através de autorizada oficial do fabricante em território nacional;
- c) junto ao contratado.

5.4.5. Serão disponibilizados, no mínimo, os seguintes meios de abertura de chamados de suporte técnico:

- a) e-mail;
- b) contato telefônico.

5.4.6. O suporte técnico deverá ter no mínimo o tempo de resposta para os níveis de severidade com base nos seguintes critérios:

- a) **Crítico:** significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno;
- b) **Alta:** impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
- c) **Média:** Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

d) Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial;

5.4.7. Deverá ser fornecido suporte completo a todas as funcionalidades da solução entregue, independentemente da funcionalidade estar ou não descrita no edital de contratação, quando solicitado pelo contratante;

5.4.8. O processo de instalação de novas versões de software, incluindo correções, é de responsabilidade da contratada e incluirá, mas não limitado a(o):

5.4.8.1. Levantamento de requisitos para a instalação e a avaliação do possível impacto no ambiente operacional e nas aplicações de produção; Certificação da compatibilidade entre os itens de software e hardware que compõe o ambiente (matriz de compatibilidade); Validação final do funcionamento normal do ambiente de produção, além de eventuais correções, quando necessário;

5.4.9. Os procedimentos corretivos de instalação das atualizações e novas versões de software deverão ser previamente agendados junto ao Órgão Responsável, que definirá a data do início dos trabalhos, acompanhará e validará os respectivos serviços, que deverão ser finalizados em prazo não superior a 60 dias após o seu início, exceto por conveniência do contratante;

5.4.10. Durante o prazo de garantia serão fornecidos e instalados, sem ônus adicional, os pacotes de correções, incluindo "patches", atualizações de software, além de novas versões de softwares da solução que corrijam problemas identificados pela fabricante;

5.4.11. Todas as intervenções realizadas no ambiente de produção e testes pelo(s) técnico(s) certificado(s) são de responsabilidade da contratada, cabendo-lhe responder por quaisquer danos porventura decorrentes dessas intervenções, bem como pela divulgação não autorizada e indevida de quaisquer dados ou informações contidas no ambiente do contratante;

5.4.12. Os chamados abertos até o último dia da vigência do contrato deverão ser solucionados, sem ônus adicional para a contratante, ainda que expirado o prazo de vigência do contrato.

5.5. REQUISITOS TEMPORAIS (IN SGD/ME Nº 94/2022 - Art. 16, inciso I, alínea e)

5.5.1. Modalidade de 24x7 para definição do horário de abertura de chamado e atendimento, ou seja, vinte quatro horas por dia e sete dias por semana, com tempo de solução descritas na tabela de severidade do chamado.

5.5.2. Deverá ser fornecido serviço de atendimento 24x7 através de linha telefônica do fabricante ou da autorizada oficial do fabricante em território nacional para abertura e gerenciamento de chamados técnicos e suporte de Software.

5.5.3. O prazo de garantia dos produtos serão de 60 (sessenta) meses, para *hardware* e *software*, a partir de seu recebimento definitivo, atendimento 24x7 para abertura de chamados e com tempo de solução conforme a tabela de severidade.

5.5.4. Todos os itens deverão serem entregues no local indicado em até 60 (sessenta) dias corridos, a contar da data de abertura da Ordem de Serviço.

Local de entrega da solução:

Unidade de Patrimônio

Hospital das Clínicas da UFMG

Avenida Alfredo Balena, 110 - Santa Efigênia

CEP: 30130-100

5.5.5. A entrega dos equipamentos pela transportadora deverá ser previamente comunicada à unidade de patrimônio do hospital com no mínimo 2 (dois) dias úteis de antecedência.

5.5.6. Para definição de dia/hora útil, considera-se de segunda a sexta-feira de 08h00h às 17h00h, horário local de Brasília, excetuando-se feriados nacionais ou da localidade, quando houver.

5.6. REQUISITOS DE SEGURANÇA (IN SGD/ME Nº 94/2022 - Art. 16, inciso I, alínea f)

5.6.1. Deverá possuir mecanismos de segurança que garantam a disponibilidade, integridade, confidencialidade e autenticidade das configurações.

5.6.2. Deverá possuir solução de gerência que permita gerenciar diferentes perfis de acesso, com autenticação por usuário e senha.

- 5.6.3. Deverá gerar registros de logs das ações de administração e eventos relevantes.
- 5.6.4. Deverá possuir recursos que permitam o monitoramento automático de eventos relevantes da solução de firewall.
- 5.6.5. Os empregados ou prestadores de serviço à serviço da contratada deverão seguir as normas de acesso às dependências físicas do contratante, sendo obrigatório o uso de crachás de identificação e, caso necessário, equipamentos de proteção individual;
- 5.6.6. O acesso às dependências da contratante, quando fora horário comercial, deve ser previamente solicitado, com antecedência mínima de 24 (vinte quatro) horas, através de contato via e-mail, com descritivo das pessoas que prestarão o serviço, exceto em situações extremas de indisponibilidade dos serviços da contratante.

5.7. REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS (IN SGD/ME Nº 94/2022 - Art. 16, inciso I, alínea g)

- 5.7.1. Deverá a execução do objeto ser realizada de acordo com os critérios de sustentabilidade ambiental contidos no art. 5º da Instrução Normativa nº 01, de 19 de janeiro de 2010, da então Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MPOG e no Decreto nº 7.746, de 05 de junho de 2012, da Casa Civil da Presidência da República, no que couber.
- 5.7.2. Deverão, preferencialmente, utilizar recursos tecnológicos que proporcionem o menor consumo de energia.
- 5.7.3. Deverão as configurações dos hardwares e dos softwares serem realizadas visando alto desempenho com a utilização racional de energia.
- 5.7.4. Deverão, preferencialmente, acondicionar os equipamentos em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.
- 5.7.5. Deverá apresentar Certificado de Rotulagem Ambiental emitido pela ABNT ou certificado emitido por organismo acreditado Cgcre (INMETRO) que assegure a conformidade com a Diretiva RoHS ou Autodeclaração do fabricante de conformidade atestando a conformidade com a Diretiva RoHS.
- 5.7.6. Deverá a CONTRATADA observar as normas, procedimentos e boas práticas relativas à prestação do serviço, se abstendo de propor soluções danosas e não usuais de mercado, assumindo ainda toda responsabilidade pelos descartes adequados de resíduos, quando da troca e reposição de peças que se fizerem necessárias.
- 5.7.7. Deverá a CONTRATADA respeitar as Normas Brasileiras - NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos.
- 5.7.8. Deverá a CONTRATADA contribuir para a promoção do desenvolvimento nacional sustentável no cumprimento de diretrizes e critérios de sustentabilidade ambiental, de acordo com o art. 225 da Constituição Federal/88.
- 5.7.9. A CONTRATADA, de maneira isolada ou em parceria com o fabricante, deverá providenciar o recolhimento e o adequado descarte dos produtos e materiais inservíveis originários da contratação, recolhendo-os aos pontos de coleta ou centrais de armazenamentos mantidos pelo respectivo fabricante ou importador, para fins de sua destinação final ambientalmente adequada, nos termos da Instrução Normativa IBAMA nº 01, de 18/03/2010, da Lei nº 12.305, de 2010 – Política Nacional de Resíduos Sólidos, Resolução CONAMA nº 416, de 30/09/2009, e legislação correlata.
- 5.7.10. A abertura de chamados técnicos e encaminhamentos de demandas, bem como todos os relatórios e artefatos produzidos deverão ser realizados, preferencialmente, sob a forma eletrônica, evitando-se a impressão de papel.
- 5.7.11. Os profissionais em atendimento no ambiente da Ebserh, deverão se apresentar devidamente identificados e vestidos de forma adequada ao ambiente de trabalho, com uniforme do fornecedor ou fabricante, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da Rede Ebserh.
- 5.7.12. Os profissionais da CONTRATADA deverão dispor de todos os equipamentos de proteção individual (EPIs), necessários à prestação dos serviços nas dependências do HC-UFMG/Ebserh.
- 5.7.13. Os profissionais da CONTRATADA deverão respeitar todos os colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo.
- 5.7.14. A CONTRATADA deverá substituir imediatamente aquele profissional que seja considerado inconveniente à boa ordem ou que venha a transgredir as normas disciplinares da Ebserh, quando solicitado

pelo HC-UFMG/Ebserh.

5.7.15. O acesso às instalações do HC-UFMG/Ebserh onde serão realizados os serviços deverá ser controlado e permitido somente às pessoas autorizadas.

5.7.16. A CONTRATADA deverá acatar e obedecer às normas e políticas internas do HC-UFMG/Ebserh.

5.7.17. A CONTRATADA deverá garantir a segurança das informações oriundas do HC-UFMG/Ebserh e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido no curso da prestação dos serviços, a menos que autorizado formalmente para tal.

IN SGD/ME Nº 94/2022 - ART. 16 INCISO II

5.8. **REQUISITOS DE ARQUITETURA TECNOLÓGICA** (IN SGD/ME Nº 94/2022 - Art. 16, inciso II, alínea a)

5.8.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN;

5.8.2. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

5.8.3. O equipamento fornecido deve ser próprio para montagem em rack 19", incluindo kit tipo trilho para adaptação, se necessário, e cabos de alimentação;

5.8.4. Devem ser fornecidos 8 (oito) módulos GBIC SFP+ 10Gbase-SR, multimodo, para uso na plataforma de segurança solicitada e nos switches da marca HPE modelo TOR FlexFabric 5900 JG838A, por appliance;

5.8.5. Devem ser fornecidos 8 (oito) módulos GBIC SFP+ 10Gbase-LR, monomodo, para uso na plataforma de segurança solicitada e nos switches da marca HP modelo TOR FlexFabric 5900 JG838A, por appliance;

5.8.6. Deve possuir throughput de, no mínimo, 8 (oito) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;

5.8.7. Deve possuir throughput de, no mínimo, 4 (quatro) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;

5.8.8. Deve suportar, no mínimo, 900.000 (novecentos mil) conexões simultâneas;

5.8.9. Deve suportar, no mínimo, 90.000 (noventa mil) novas conexões por segundo;

5.8.10. Deve possuir, no mínimo, 12 (doze) interfaces físicas de rede de 1 Gbps do tipo RJ-45;

5.8.11. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 1 Gbps do tipo SFP;

5.8.12. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 10 Gbps do tipo SFP+;

5.8.13. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento;

5.8.14. Deve possuir, no mínimo, 1 (uma) interface física dedicada para o recurso de alta disponibilidade;

5.8.15. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;

5.8.16. Deve possuir, no mínimo, 120 (cento e vinte) GB de armazenamento interno para o sistema operacional e registro de logs;

5.8.17. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento (hot-swappable);

5.8.18. Deve suportar, no mínimo, 1.000 (um mil) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;

5.8.19. Deve suportar, no mínimo, 500 (quinhentos) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;

5.8.20. Deve estar licenciado e habilitado para uso ilimitado de usuários e endereços de rede;

5.8.21. Deve possuir suporte a criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 1.000 (um mil) VLANs;

- 5.8.22. Deve implementar o protocolo LLDP – Link Layer Discovery Protocol;
- 5.8.23. Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um link agrupado virtualmente (LAG – Link Aggregation Group);
- 5.8.24. Deve possuir o recurso de NAT – Network Address Translation nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso deve ser aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (Network Prefix Translation) para tradução de um prefixo IPv6 para outro prefixo IPv6 prevenindo problemas de roteamento assimétrico;
- 5.8.25. Deve suportar a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF graceful restart e BGP;
- 5.8.26. Deve implementar o protocolo ECMP – Equal Cost Multiple Path para balanceamento de carga entre links baseados no hash do endereço IP de origem, no hash do endereço IP de origem e de destino, pela técnica conhecida como round-robin e com base no peso ou prioridade atribuído a cada link. Deve suportar o balanceamento entre, no mínimo 4 (quatro) links;
- 5.8.27. Deve permitir o envio de logs para sistemas de monitoração externos utilizando o padrão syslog, bem como o envio de forma segura através do protocolo SSL/TLS;
- 5.8.28. Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo, com a sincronização dos seguintes itens:
- I - sessões;
 - II - configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
 - III - certificados descryptografados;
 - IV - associações de segurança das VPNs;
 - V - tabelas de roteamento;
- 5.8.29. O recurso de alta disponibilidade poderá atuar nos modos ativo/passivo ou ativo/ativo, A solução deverá possuir suporte ao recurso de VLAN (IEEE 802.1q), com no mínimo 4094 (quatro mil e noventa e quatro) VLANs;
- 5.8.30. Atuar como servidor DHCP e retransmissor (relay) DHCP e ter o recurso de DHCP cliente;
- 5.8.31. Deve implementar controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego;
- 5.8.32. A identificação do país deve ser através do código do país, por exemplo, BR, USA, UK, RUS, etc e também através de geolocalização possibilitando a criação de regiões geográficas;
- 5.8.33. Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;
- 5.8.34. Deve possuir a capacidade para realizar a descryptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A descryptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego;
- 5.8.35. Deve possuir recurso de QoS – Quality of Service com suporte a DSCP – Differentiated Services Code Point. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação;
- 5.8.36. Deve possuir a capacidade de reconhecer, no mínimo, 3.000 (três mil) aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, peer-to-peer, sistemas de mensagem instantânea, etc, sendo esta uma lista não exaustiva;
- 5.8.37. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, emule, skype, teams, facebook, linkedin, twitter, whatsapp, citrix, vmware, hyper-v, logmein, teamviewer, anydesk, ammyy, ms rdp, vnc, gmail, outlook, youtube, http-tunnel, facebook chat, gmail chat, 4shared, dropbox, google drive, onedrive, db2, mysql, postgresql, sql server, kerberos, ldap, radius, itunes, dhcp, ftp, ssh, dns, wins, msrpc, ntp, snmp, webex;
- 5.8.38. Deve permitir o bloqueio total de aplicações proxies (exemplo: Ultrasurf, GPass, FreeGate, Hopster, Tor, HotSpot Shield);

- 5.8.39. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 5.8.40. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos, os seguintes ataques conhecidos: SQL injection, ICMP denial of service, força bruta e scanning de portas, CIFS, Port overflow, Non compliant SSL, IKE aggressive exchange;
- 5.8.41. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 5.8.42. Identificar e bloquear comunicação com botnets;
- 5.8.43. Detectar e bloquear a origem de portscans, permitindo a criação de exceções para endereços IPs de ferramentas de monitoramento da instituição;
- 5.8.44. Suportar o monitoramento de arquivos trafegados na internet (HTTP, HTTPS, FTP, SMTP), assim como arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação;
- 5.8.45. Permitir a visualização dos resultados das análises de malwares do tipo zero day nos diferentes sistemas operacionais suportados;
- 5.8.46. Deverá possuir ferramenta de diagnóstico do tipo tcpdump;
- 5.8.47. Deverá oferecer a proteção conhecida como URL filtering, que analisa cada URL acessada pelos usuários. Esta proteção é importante para ajudar o usuário a se proteger ao acessar sites desconhecidos, evitando assim ataques de phishing. Em relação à essa proteção o firewall deverá atender aos seguintes requisitos: suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL, classificar o nível de risco de URLs em níveis, classificar sites em mais de uma categoria, a categorização de URL deve analisar toda a URL e não somente até o nível de diretório e bloquear o acesso do usuário caso esse tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;
- 5.8.48. Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica (HTTPS), quanto em CLI (linha de comando: SSH);
- 5.8.49. O reconhecimento da aplicação se dará, independentemente de porta e protocolo, através de, no mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da solução de firewall, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado;
- 5.8.50. Deve permitir a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante;
- 5.8.51. Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação;
- 5.8.52. Deve permitir bloquear sessões TCP que utilizarem variações do three-way handshake como four-way e o five-way split handshake, prevenindo assim possíveis tráfegos maliciosos;
- 5.8.53. Deve permitir bloquear conexões que contenham dados no payload dos pacotes TCP SYN e TCP SYN-ACK durante o three-way handshake;
- 5.8.54. A solução de firewall deve possuir funcionalidades de IPS, antivírus e anti-spyware que permita o bloqueio de vulnerabilidades e exploits conhecidos e proteção contra vírus e spywares baseado em assinaturas de ameaças conhecidas;
- 5.8.55. Deve ser possível a criação de assinaturas customizadas de ameaças;
- 5.8.56. Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de appliance externo para o bloqueio de vírus caso a solução de firewall ofertada não realize nativamente a inspeção em algum dos protocolos solicitados;
- 5.8.57. Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;
- 5.8.58. Deve possuir funcionalidade para análise de ameaças de comando e controle desconhecidas, sendo capaz de monitorar e bloquear a comunicação em tempo real através de HTTP, SSL, aplicações desconhecidas de tráfego TCP e UDP;
- 5.8.59. Deve possuir proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN Flood, ICMP Flood, UDP Flood, etc e deve também bloquear port scans, bloquear ataques de buffer overflow e identificar e bloquear comunicação com botnets;

5.8.60. Para cada ameaça detectada pela solução deve ser realizado o registro nos logs do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego);

5.8.61. A solução de firewall deve possuir funcionalidade para análise de ameaças de comando e controle desconhecidas, sendo capaz de monitorar e bloquear a comunicação em tempo real através de HTTP, SSL, aplicações desconhecidas de tráfego tanto TCP quanto UDP;

5.8.62. A solução de firewall deve possuir a capacidade de detectar e bloquear tentativas de resolução de domínios gerados de forma automática através de algoritmos (Domain Generation Algorithm - DGA);

5.8.63. A solução de firewall deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle. A análise automática deve incluir, no mínimo, as seguintes características:

- I - Padrões de consulta;
- II - Entropia;
- III - Análise de frequência n-gram de domínios;
- IV - Taxa de consultas.

5.8.64. A solução de firewall deve possuir funcionalidade para análise de malwares não conhecidos (Malware Zero Day) onde o dispositivo envia o arquivo de forma automática para análise na "cloud" ou em um appliance instalado na rede local onde o arquivo será executado e simulado em um ambiente controlado (sandbox);

5.8.65. Caso seja fornecido um appliance local para análise de malwares não conhecidos ele deve possuir, no mínimo, 28 (vinte e oito) ambientes controlados (sandbox) independentes para execução simultânea de arquivos suspeitos;

5.8.66. Caso seja necessário licença de sistema operacional e software para execução de arquivos no ambiente controlado (sandbox) as mesmas devem ser fornecidas em sua totalidade para o seu perfeito funcionamento;

5.8.67. O resultado da análise de malwares não conhecidos deve ter a capacidade de categorizar o arquivo analisado como, no mínimo, um arquivo malicioso, um arquivo não malicioso e um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema;

5.8.68. A análise de malwares não conhecidos deve ser realizada em arquivos trafegados na internet através dos protocolos HTTP, HTTPS e FTP bem como em arquivos trafegados entre servidores de arquivos utilizando o protocolo SMB. A análise também deve ser realizada em arquivos anexos em e-mails e links HTTP e HTTPS presentes no corpo de e-mails trafegados utilizando os protocolos SMTP e POP3. A análise do link HTTP e HTTPS presente no corpo do e-mail deve identificar se o website é um hospedeiro de exploits ou atividade de phishing;

5.8.69. Deve suportar a análise dos arquivos em ambientes controlados (sandbox) com, no mínimo, os sistemas operacionais MS Windows, MacOS e Linux;

5.8.70. A análise de malwares não conhecidos em ambiente controlado (sandbox) deve ser realizada em arquivos tipo executáveis, DLLs, arquivos compactados RAR e 7-ZIP, arquivos do pacote MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos PDF, arquivos JAVA (.jar e class), arquivos DMG e PKG, arquivos ELF e arquivos APK;

5.8.71. Deve atualizar a base de assinaturas para bloqueio dos malwares identificados no ambiente controlado (sandbox) dentro de, no máximo, 5 (cinco) minutos;

5.8.72. A solução de firewall deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a websites baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP;

5.8.73. A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;

5.8.74. Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;

5.8.75. Deve prover análise em tempo real dos websites acessados pelos usuários realizando a inspeção do seu conteúdo, detectando assim conteúdos que possam ser uma ameaça e realizando a

categorização da URL como maliciosa e bloqueando tal URL, mesmo que ela não esteja presente e devidamente categorizada na base de dados de URL da solução;

5.8.76. Deve permitir a customização da página de bloqueio exibida ao usuário quando o mesmo tentar realizar um acesso a um website pertencente a uma categoria de URLs bloqueada;

5.8.77. Deve possuir recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o Active Directory, submetidas em sites não corporativos. Deve ser possível definir em quais websites é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o website pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao Active Directory em um website não autorizado deve ser exibido no web browser do mesmo uma página de bloqueio informando que o uso de tais credenciais no website específico não está autorizado;

5.8.78. A solução de firewall deve possuir recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e também definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de web browser. Deve permitir bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent;

5.8.79. A solução de firewall deve possuir integração com LDAP, MS Active Directory e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas/regras baseadas por usuários e grupo de usuários;

5.8.80. A integração com MS Active Directory para identificação dos usuários da rede deve ser realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários;

5.8.81. Deve suportar autenticação para smartphones e tablets;

5.8.82. A solução de proteção de rede contará com recurso de filtro de URL ou filtro web que permita definir políticas/regras por tempo, por usuários e grupos de usuários do protocolo LDAP/AD, endereços IPs e redes de endereços IPs;

5.8.83. Quanto ao recurso de filtro de URL, a solução deverá ser capaz de customizar a página de bloqueio exibida ao usuário;

5.8.84. A solução de firewall deve possuir recurso de portal de autenticação prévia (Captive Portal) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de software cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;

5.8.85. A solução de firewall deve possuir o recurso de VPN – Virtual Private Network dos tipos site-to-site e client-to-site e suportar IPSEC – Internet Protocol Security e SSL – Secure Sockets Layer;

5.8.86. O recurso de VPN IPSEC deve suportar os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5 e SHA 1, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14 e suportar também a autenticação através de certificados IKE PKI;

5.8.87. O recurso de VPN SSL deve permitir que o usuário remoto se conecte através de um software cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo;

5.8.88. Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a autenticação via certificado e OTP – One Time Password;

5.8.89. Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional MS Windows 10, MS Windows 11, MacOS e Linux e para instalação em dispositivos móveis Android e IOS;

5.8.90. O recurso de VPN SSL deve possuir mecanismo de checagem da conformidade do computador do usuário remoto e a checagem deve permitir verificar, no mínimo, as informações de qual sistema operacional e patches estão instalados, se o antivírus está instalado e ativo no computador, se o firewall está instalado e ativo no computador, se o disco está criptografado, se o agente de DLP – Data Loss Prevention está instalado e ativo, informações de chaves de registro e processos ativos no computador;

5.8.91. Deve ser possível criar perfis customizados de conformidade com, no mínimo, as mesmas informações obtidas pelo mecanismo de checagem da conformidade do computador do usuário remoto. Tais perfis devem ser utilizados para assegurar que apenas computadores de usuários remotos que atendem

aos requisitos solicitados nos perfis customizados possam ter acesso através da VPN aos dados e sistemas hospedados na rede interna do órgão;

5.8.92. A solução de firewall deve possuir console de gerenciamento do equipamento acessada através de interface gráfica web permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e anti-spyware, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de logs de eventos e demais configurações;

5.8.93. Deve suportar a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS Active Directory, RADIUS e através de base de usuários local no equipamento da solução de firewall;

5.8.94. Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros;

5.8.95. Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;

5.8.96. A interface de gerenciamento do equipamento deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regras (shadowing) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve possuir também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão da mesma para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente. É permitido o uso de appliance externo para realização da análise das políticas, devendo o mesmo ser fornecido em conjunto com a solução de firewall e estar devidamente licenciado;

5.8.97. Deve ser possível através de interface de gerenciamento do equipamento a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuário específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados;

5.8.98. Deve ser possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – Software as a Service mostrando os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso a aplicação SaaS e o consumo da aplicação SaaS pelo usuário;

5.8.99. Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;

5.8.100. Deve ser possível configurar o envio de alertas do sistema via e-mail;

5.8.101. Deve suportar o monitoramento via SNMPv3;

5.8.102. Implementar mecanismo de sincronismo de horário através do protocolo NTP;

5.8.103. Permitir a configuração de multi WAN, possibilitando ao menos 2 (duas) conexões externas com a internet simultaneamente, além de prover balanceamento de enlace de conexão por:

- I - resumo criptográfico do endereço IP de origem,
- II - resumo criptográfico do endereço IP de origem e destino,
- III - pela técnica conhecida como round-robin,
- IV - por peso ou prioridade,
- V - por políticas de usuários e grupos de usuários de serviços baseados no protocolo LDAP, como o Microsoft Active Directory, e
- VI - através de políticas de aplicação e porta de destino;

5.8.104. O sistema operacional a ser instalado no equipamento que compõe a solução deverá ser fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico;

5.8.105. Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

5.8.106. A Solução de Firewall ofertada deve ser homologada e totalmente compatível com o software de gerenciamento centralizado Palo Alto Panorama atualmente instalado e em uso no HC-UFMG;

5.8.107. Na data do certame, nenhum dos equipamentos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

5.8.108. Durante o período de vigência do contrato de garantia todos os componentes da solução de firewall, incluindo o equipamento, o sistema operacional do mesmo, as licenças necessárias para atender as funcionalidades e recursos solicitados, os softwares clientes de VPN e demais itens necessários para o perfeito funcionamento devem estar cobertos por garantia e suporte técnico do fabricante da solução em caso de problema;

5.8.109. A solução de firewall deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais software e das assinaturas de proteção da solução.

5.8.110. Implementar o controle, inspeção, e descryptografia do padrão SSL e SSH nos tráfegos de entrada e saída;

5.8.111. Possibilitar a modelagem de tráfego (traffic shapping) e as técnicas de qualidade de serviço (QoS) com base em políticas/regras, tais como prioridade, garantia e valor máximo, bem como marcação de pacotes, inclusive por aplicações, permitindo a limitação de consumo de banda (envio e recebimento) baseados no endereço IP de origem ou destino, aplicações, porta, usuários e grupos de usuários com base no protocolo LDAP/AD;

5.9. **SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL** (IN SGD/ME Nº 94/2022 - Art. 16, inciso II, alíneas "b" e "c")

Características técnicas mínimas:

5.9.1. A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:

I - Reunião de alinhamento para criação do escopo do projeto previamente a instalação;

II - Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante. Deve considerar também a instalação em modo Alta Disponibilidade (ativo/passivo);

III - Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados;

IV - Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

V - Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;

VI - Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

VII - Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e Anti-malware de acordo com as exigências levantadas;

5.9.2. Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls afim de garantir a melhor eficiência da solução durante o período de vigência das licenças;

5.9.3. As atividades de configuração da solução, migração de regras e demais atividades necessárias para a configuração do sistema poderão ser realizadas de forma remota;

5.9.4. Adição do novo appliance de firewall ao sistema de gerenciamento centralizado Palo Alto Panorama atualmente instalado e em uso no HC-UFGM;

5.9.5. Repasse de informação das configurações realizadas no formato hands-on de 4 horas para a equipe responsável pelo projeto por parte da contratante após validação da migração;

5.9.6. **DA CONCLUSÃO DA IMPLANTAÇÃO**

5.9.6.1. Após a conclusão da implantação da solução (entrega, instalação e configuração), a CONTRATADA disponibilizará ao HC-UFGM a documentação final do projeto, completa e atualizada, de modo a sinalizar a conclusão da etapa de implantação e solicitará a validação para fins de recebimento definitivo.

5.9.6.2. O HC-UFMG/Ebserh avaliará todos os aspectos relacionados ao fornecimento e implantação da solução e, caso todos os requisitos tenham sido atendidos, emitirá o Termo de Recebimento Definitivo.

ANEXO VII - (MODELO DO TERMO DE RECEBIMENTO DEFINITIVO).

5.9.6.3. Todas as fases e prazos estão contidas na tabela *Tabela 01 – cronograma de execução do contrato* do item 7.1.7 desse Termo de Referência.

5.10. IDENTIFICAÇÃO DAS DEMAIS NECESSIDADES

5.10.1. A empresa contratada para entregar a solução deverá possuir experiência na implantação do tipo de solução de proteção de rede, justificando-se tal requisito para que a empresa contratada para implantar a solução possua expertise e pessoal técnico qualificado para isso;

5.10.2. A empresa contratada para entregar a solução deve possuir parceria oficial com a fabricante ou fornecedora da solução a mais de 2 anos;

5.10.3. A solução deverá ser implantada através do uso de equipamentos novos e sem uso, não sendo aceitos equipamentos usados, remanufaturados ou de demonstração, bem como não deverá ser composta por equipamentos listados ou previstos na listagem do fabricante em listas de "end-of-life" ou "end-of-sale" no momento da apresentação da proposta;

5.10.4. Os equipamentos que compõem a solução de proteção de rede, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante;

5.10.5. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a contratada sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à contratante a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

5.10.6. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante da solução. Em momento anterior à instalação, o contratante poderá solicitar os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços, sendo direito da mesma a sua aceitação, ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas;

5.10.7. A realização do serviço de implantação deve ser planejada de acordo com disponibilidade do contratante. O planejamento anterior ao serviço deverá ser realizado de forma **on-site nas dependências do contratante**;

5.10.8. Ao término dos serviços de implantação deverá ser entregue um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 dias após a finalização dos serviços;

5.10.9. Os funcionários da contratada deverão possuir todo o ferramental necessário ao exercício das suas atividades;

5.10.10. Todas as atualizações de firmware ou qualquer outro software componente da solução deverão estar na versão mais atualizada disponível;

5.10.11. Criar templates de relatórios sobre;

a) Volume total de conexões que foram bloqueadas e liberadas;

b) Conexões bloqueadas, seus destinos e serviços;

c) Principais regras que possuem tráfego de rede alto;

d) Principais ataques detectados e suas origens e destinos;

e) Principais eventos, origens, destinos e serviços;

f) Sites mais acessados;

g) E demais informações que o contratante julgar necessário no momento da implantação.

Durante toda implantação e configuração, o responsável pela solução de proteção de rede demonstrará à equipe de tecnologia da informação do contratante, como instalar e configurar os equipamentos e softwares que compõem a solução, através de implantação assistida.

5.11. REQUISITOS DE GARANTIA E MANUTENÇÃO (IN SGD/ME Nº 94/2022 - Art. 16, inciso II, alínea "d")

São os mesmos requisitos do item 5.4, aqui replicados.

5.11.1. Entende-se como manutenção as atividades relativas ao bom funcionamento da solução que abrangem: garantia de funcionamento, suporte técnico e atualização da solução;

5.11.2. A contratada deverá prestar garantia de funcionamento, suporte técnico e atualização pelo período de 60 meses, contados da data do aceite definitivo da instalação, configuração e ativação da solução. É de responsabilidade da contratada garantir que o suporte padrão de 60 meses registrado junto ao fabricante abranja todo o período contratado, atendido no local da instituição (on-site), com atendimento durante 24 horas, nos sete dias da semana (24x7), abrangendo-se todo e qualquer defeito, desde seu projeto, fabricação e desempenho dos equipamentos e serviços de segurança inclusos na solução;

5.11.3. Em caso de defeitos de fabricação, o serviço de garantia incluirá o envio de peças ou equipamentos de reposição nos locais apontados no instrumento licitatório, no mínimo na modalidade NDB (Next Business Day);

5.11.4. O suporte técnico será acionado:

- a) junto ao fabricante da solução de proteção de rede;
- b) através de autorizada oficial do fabricante em território nacional;
- c) junto ao contratado.

5.11.5. Serão disponibilizados, no mínimo, os seguintes meios de abertura de chamados de suporte técnico:

- a) página web;
- b) e-mail;
- c) contato telefônico.

5.11.6. O suporte técnico deverá ter no mínimo o tempo de resposta para os níveis de severidade com base nos seguintes critérios:

- a) Crítico: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno;
- b) Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
- c) Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
- d) Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial;

5.11.7. Deverá ser fornecido suporte completo a todas as funcionalidades da solução entregue, independentemente da funcionalidade estar ou não descrita no edital de contratação, quando solicitado pelo contratante;

5.11.8. O processo de instalação de novas versões de software, incluindo correções, é de responsabilidade da contratada e incluirá, mas não limitado a(o):

5.11.8.1. Levantamento de requisitos para a instalação e a avaliação do possível impacto no ambiente operacional e nas aplicações de produção; Certificação da compatibilidade entre os itens de software e hardware que compõe o ambiente (matriz de compatibilidade); Validação final do funcionamento normal do ambiente de produção, além de eventuais correções, quando necessário;

5.11.9. Os procedimentos corretivos de instalação das atualizações e novas versões de software deverão ser previamente agendados junto ao Órgão Responsável, que definirá a data do início dos trabalhos, acompanhará e validará os respectivos serviços, que deverão ser finalizados em prazo não superior a 60 dias após o seu início, exceto por conveniência do contratante;

5.11.10. Durante o prazo de garantia serão fornecidos e instalados, sem ônus adicional, os pacotes de correções, incluindo "patches", atualizações de software, além de novas versões de softwares da solução que corrijam problemas identificados pela fabricante;

5.11.11. Todas as intervenções realizadas no ambiente de produção e testes pelo(s) técnico(s) certificado(s) são de responsabilidade da contratada, cabendo-lhe responder por quaisquer danos

porventura decorrentes dessas intervenções, bem como pela divulgação não autorizada e indevida de quaisquer dados ou informações contidas no ambiente do contratante;

5.11.12. Os chamados abertos até o último dia da vigência do contrato deverão ser solucionados, sem ônus adicional para a contratante, ainda que expirado o prazo de vigência do contrato.

5.12. **DA RETIRADA DOS EQUIPAMENTOS EM CASO DE ACIONAMENTO DE GARANTIA OU TROCA DE PEÇAS:**

5.12.1. A retirada de equipamentos pela CONTRATADA deverá ocorrer em até 5 dias úteis a contar da solicitação, devendo o ato da retirada ser previamente comunicado ao HC-UFMG/Ebserh, com no mínimo 2 (dois) dias úteis de antecedência à retirada.

5.12.2. A responsabilidade do serviço de remoção, logística e embalagem dos equipamentos para transporte é da CONTRATADA.

5.13. **REQUISITOS DE CAPACITAÇÃO (IN SGD/ME Nº 94/2022 - Art. 16, inciso II, alínea "e")**

5.13.1. Os serviços de capacitação técnica deverão contemplar a explanação teórica e prática (configuração, operação da solução de firewall e gerência) para administradores da solução;

5.13.2. O treinamento para a equipe de tecnologia da informação deverá ser realizado em formato presencial com duração mínima de 04 horas;

5.13.3. O treinamento deverá ser realizado antes da entrada em produção dos equipamentos;

5.13.4. A capacitação técnica deve ser realizada nas dependências da contratante, com carga horária mínima de 04 horas, em data e horário a ser definido entre as partes;

5.13.5. **O treinamento deve oferecer em seu escopo:**

5.13.5.1. Informativo dos componentes tecnológicos que foram adquiridos na solução;

5.13.5.2. Compreensão de todo o funcionamento e operação da solução adquirida;

5.13.5.3. Características e funcionamento de todos os módulos envolvidos na composição do firewall, sendo importante o repasse de conhecimento e usabilidade de todos estes módulos de forma completa para utilização por parte do contratante de toda tecnologia entregue.

5.13.6. **O treinamento deverá contemplar no mínimo o conteúdo abaixo:**

5.13.6.1. Instalação e configuração básica do equipamento e gerência, incluindo configuração das interfaces, NTP, DNS, atualização de assinaturas, etc;

5.13.6.2. Configuração de alta disponibilidade e teste de funcionamento da mesma;

5.13.6.3. Criação e verificação de regras de firewall;

5.13.6.4. Criação e verificação de políticas de NAT;

5.13.6.5. Descriptografia;

5.13.6.6. Sandboxing de ameaças avançadas;

5.13.6.7. Integração de autenticação com Active Directory;

5.13.6.8. Configuração e verificação de políticas de IPS, anti-bot, anti-vírus, controle de aplicação e filtro de URL;

5.13.6.9. Configuração de filtro de conteúdo e customização de página de bloqueio;

5.13.6.10. Configuração de VPN site-to-site;

5.13.6.11. Configuração de VPN client-to-site;

5.13.6.12. Configuração de VPN SSL;

5.13.6.13. Backup e restore de configuração;

5.13.6.14. Disaster recovery;

5.13.6.15. Atualização de firmware;

5.13.6.16. Monitoramento, criação e customização de relatórios;

5.13.7. **Material didático**

5.13.8. Será dispensada o fornecimento de material didático em meio físico;

5.13.9. Necessário informar os melhores canais de consulta de materiais, como sites do fabricante, fóruns, etc.

5.14. **REQUISITOS DE EXPERIÊNCIA PROFISSIONAL (IN SGD/ME Nº 94/2022 - Art. 16, inciso II, alínea "f")**

5.14.1. Os profissionais componentes da equipe de implantação da solução deverão ser devidamente qualificados pelo fabricante da solução ou pela contratada, sendo tal comprovação feita por meio de

apresentação de certificados de capacitação emitidos e nome do profissional.

5.15. REQUISITOS DE FORMAÇÃO DA EQUIPE DE PROJETO, IMPLEMENTAÇÃO E IMPLANTAÇÃO (IN 01/2019 SGD/ME – Art. 16, inciso II, alínea g)

5.15.1. Deverá se apresentado um Preposto, nos termos da alínea "a", inciso II do artigo 17 da IN 94 da SGD/ME e do Art. 162 do Regulamento de Licitações e Contratos da Ebserh - RLCE, aceito pela Administração, para representar a CONTRATADA ao longo da execução contrato.

5.15.2. Deverá ser apresentado um Gerente de Projetos (podendo este ser o Preposto), que será o ponto focal para tratativas de assuntos relativos à execução dos serviços, sendo este o responsável por coordenar e orientar todos os técnicos para execução dos serviços, de forma que os prazos e qualidade estabelecidos sejam respeitados. Caberá ainda ao Gerente de Projetos apresentar na reunião uma lista de contatos de comunicação para esclarecimento de dúvidas ou apoio de itens relacionados ao projeto.

5.15.3. O serviço de instalação e configuração devem ser realizados por técnicos certificados, com capacidade técnica para a realização do serviço, comprovado através da apresentação de documento de certificação emitido pelo fabricante do equipamento ou por empresa de treinamento reconhecida pelo fabricante.

5.15.4. O suporte técnico em garantia deve ser realizado por profissionais devidamente habilitados, treinados e qualificados na solução ofertada.

5.16. REQUISITOS DE METODOLOGIA DE TRABALHO (IN 01/2019 SGD/ME – Art. 16, inciso II, alínea h)

5.16.1. Deverão ser adotadas as boas práticas e técnicas conhecidas de gerenciamento de projeto.

5.16.2. Os serviços de suporte técnico em garantia deverão seguir as melhores práticas preconizadas pelo ITIL.

5.17. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE (IN 01/2019 SGD/ME – Art. 16, inciso II, alínea i)

5.17.1. A CONTRATADA deverá garantir a segurança das informações do HC-UFMG/Ebserh e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido ou tido ciência no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.

5.17.2. A CONTRATADA deverá observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação - TI do HC-UFMG/Ebserh;

5.17.3. A CONTRATADA deverá manter sigilo sobre todos os ativos de informações e de processos do HC-UFMG/Ebserh, conforme itens de instrumento de confidencialidade próprio do HC-UFMG/Ebserh.

5.17.4. A CONTRATADA é integralmente responsável pela manutenção de sigilo sobre quaisquer dados e informações contidos em quaisquer documentos e em quaisquer mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto e forma divulgar, reproduzir ou utilizar.

5.17.5. A CONTRATADA deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do HC-UFMG/Ebserh ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Contrato.

5.17.6. A CONTRATADA deverá exigir de seus empregados, formalmente, o compromisso de atendimento aos regulamentos de propriedade, sigilo, confidencialidade, segurança das informações e de disciplina funcional que venha a ter conhecimento no exercício de suas atribuições, antes de autorizá-los a ingressar na execução dos serviços contratados.

5.17.7. A CONTRATADA deverá promover o afastamento imediato, após o recebimento da notificação, de qualquer dos seus profissionais que, comprovadamente, coloquem em risco as condições de preservação da propriedade, do sigilo e segurança das informações a que tiver acesso. É vedada a veiculação de publicidade acerca dos serviços contratados, sem prévia autorização por escrito do HC-UFMG/Ebserh.

5.17.8. A CONTRATADA deverá assinar o Termo de Confidencialidade **ANEXO I - (MODELO DO TERMO DE CONFIDENCIALIDADE)** entre a CONTRATADA e o HC-UFMG/Ebserh, por meio de instrumento

próprio desta, estabelecendo compromisso de não divulgar nenhum assunto tratado na prestação de serviços, do objeto da licitação.

5.17.9. O Termo de Ciência **ANEXO II - (MODELO DO TERMO DE CIÊNCIA)** deverá ser assinado por todos os empregados da CONTRATADA que estiverem diretamente envolvidos na contratação e prestação dos serviços.

5.17.10. O responsável pela implantação da solução de proteção de rede deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias dos quais venha a ter conhecimento durante a referida implantação, não podendo sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena da lei, independentemente da classificação de sigilo conferida pelo contratante a tais dados e informações.

5.18. **DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) (Ofício-Circular - SEI 3 nº 14575006)**

5.18.1. **DO TRATAMENTO DE DADOS PESSOAIS**

5.18.1.1. Em razão do objeto contratado e para seu cumprimento, a CONTRATADA realizará o tratamento de dados pessoais e dados pessoais sensíveis em nome da CONTRATANTE, nos termos do inciso VII, do artigo 5º e artigo 39, da Lei nº. 13.709, de 14 de agosto de 2018.

5.18.1.2. A CONTRATADA deve cumprir as disposições da Lei nº. 13.709, de 14 de agosto de 2018, bem como das políticas e normas internas da Empresa Brasileira de Serviços Hospitalares sobre o tema (disponíveis em www.ebserh.gov.br), implementando medidas técnicas e organizacionais adequadas para assegurar a proteção dos direitos do titular dos dados pessoais.

5.18.1.3. O tratamento de dados pessoais pela CONTRATADA será limitado às atividades estritamente necessárias para o alcance das finalidades do objeto contratado ou, quando for o caso, ao cumprimento de obrigação legal ou regulatória, ao exercício regular de direito, por determinação judicial ou por requisição da Autoridade Nacional de Proteção de Dados.

5.18.1.4. O tratamento de dados pessoais só poderá ser realizado pela CONTRATADA durante o prazo previsto para a execução do objeto contratado.

5.18.1.5. É vedado à CONTRATADA o compartilhamento dos dados pessoais com outras pessoas jurídicas ou físicas, salvo aquelas decorrentes de obrigações legais ou regulamentares necessárias para viabilizar o cumprimento do instrumento contratual ou com a prévia autorização da CONTRATANTE.

5.18.1.6. Nas hipóteses de compartilhamento previstas no item anterior, a CONTRATADA assume toda a responsabilidade decorrente da operação realizada, especialmente no que diz respeito à observância da adequada proteção e resguardo aos direitos dos titulares originais.

5.19. **DO ENVIO DA PROPOSTA**

5.19.1. Apresentar proposta comercial conforme modelo de proposta do **ANEXO V - (MODELO DA PROPOSTA DE PREÇOS)** desse Termo de Referência.

5.19.2. **Apresentar em conjunto com a proposta declaração que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa conforme exigência da RESOLUÇÃO CGPAR Nº 29, DE 5 DE ABRIL DE 2022**, bem como exigência registrada no [Acórdão n. 2.569/2018 – Plenário do TCU](#).

5.19.3. A licitante vencedora deverá apresentar, juntamente com a proposta, atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando o fornecimento de um quantitativo mínimo de uma unidade de item similar ou superior ao licitado.

5.19.4. Após a fase de lances, a licitante deverá encaminhar, no prazo fixado em edital, a contar da convocação do agente de licitação, no sistema Comprasnet:

- a) Proposta de Preços com os valores atualizados em conformidade com os lances eventualmente ofertados;
- b) Catálogo, Folder, Rótulo ou Fotografia do produto ofertado contendo as especificações técnicas;
- c) A proposta deverá ser acompanhada com o preenchimento dos requisitos do Anexo VIII - Planilha Ponto a Ponto de cumprimento de requisitos do TR (40516246);

6. **RESPONSABILIDADES (IN 94/2022 SGD/ME – ART. 17)**

6.1. **DEVERES E RESPONSABILIDADES DA CONTRATANTE (IN 94/2022 SGD/ME – Art. 17, inciso I, alíneas "a" a "h")**

- 6.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- 6.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;
- 6.1.3. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- 6.1.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
- 6.1.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- 6.1.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- 6.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável; e
- 6.1.8. 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;
- 6.2. Observar que durante a vigência do contrato sejam cumpridas as obrigações assumidas pela CONTRATADA, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas na licitação.
- 6.3. Disponibilizar a infraestrutura necessária para o fiel cumprimento das obrigações assumidas pela CONTRATADA, tais como, ponto de energia elétrica e ponto de rede lógica.
- 6.4. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta.
- 6.5. Zelar pela integridade material e funcional dos equipamentos alocados em suas dependências em função da execução dos serviços contratados.
- 6.6. Permitir acesso dos empregados da CONTRATADA às suas dependências para a execução dos serviços, observando os critérios estabelecidos neste Termo de Referência.
- 6.7. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelo representante ou preposto da CONTRATADA.
- 6.8. Fornecer condições adequadas para instalações dos equipamentos.
- 6.9. Disponibilizar local para a acomodação dos equipamentos até a instalação.

6.10. DEVERES E RESPONSABILIDADES DA CONTRATADA (IN 01/2019 SGD/ME – Art. 17, inciso II, alíneas "a" a "h")

- 6.10.1. Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato;
- 6.10.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- 6.10.3. 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;
- 6.10.4. 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;
- 6.10.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- 6.10.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- 6.10.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e
- 6.10.8. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação,

os modelos de dados e as bases de dados à Administração;

6.11. Entregar os equipamentos que compõem a solução dentro dos parâmetros e rotinas estabelecidos neste Termo de Referência e seus anexos, observando-se as normas e legislação pertinente.

6.12. Realizar a entrega dos equipamentos que compõem a solução no respectivo local de entrega, devendo prever, quando for o caso, carregadores sob sua exclusiva responsabilidade para descarregamento e entrega dos materiais até a conferência preliminar pela equipe do almoxarifado local.

6.13. Fornecer os equipamentos que compõem a solução nas embalagens originais e adotar todas as medidas preventivas no sentido de se minimizar acidentes ou danos que venham a comprometer a qualidade e a quantidade fornecida.

6.14. Responsabilizar-se por quaisquer ônus, despesas, obrigações trabalhistas, previdenciárias, fiscais, de acidentes de trabalho, bem como alimentação, transporte ou outro benefício de qualquer natureza, decorrentes da aquisição de bens e com todos os encargos sociais previstos na legislação vigente e de quaisquer outros em decorrência da sua condição de empregadora.

6.15. Assumir todos os encargos de possível demanda trabalhista, cível ou penal relacionados aos materiais, originalmente ou vinculada por prevenção, conexão ou continência.

6.16. Ser responsável por intervenções nos equipamentos que compõem a solução, que se façam necessárias, durante a vigência da garantia, sem ônus para o HC-UFMG/Ebserh. Preferencialmente, o atendimento corretivo deverá ser feito nas dependências HC-UFMG/Ebserh. Na impossibilidade, deverá existir justificativa comprovada.

6.17. Respeitar os prazos e horários das atividades de entrega, instalação, migração e repasse de conhecimento.

6.18. Durante a vigência do contrato e da garantia, a CONTRATADA deverá realizar atualizações de *firmware*, *recall* de peças ou demais intervenções que se fizerem necessárias para garantir a continuidade e qualidade do serviço, sem ônus ao HC-UFMG/Ebserh.

6.19. A CONTRATADA é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, e responderá por danos causados diretamente a terceiros ou ao HC-UFMG/Ebserh, independentemente da comprovação de sua culpa ou dolo na execução do contrato.

6.20. A CONTRATADA é responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato.

6.21. A inadimplência do contratado quanto aos encargos trabalhistas, previdenciários, fiscais e comerciais não transfere ao HC-UFMG/Ebserh a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato ou restringir a regularização e uso das obras e edificações, inclusive perante o Registro de Imóveis.

6.22. **DEVERES E RESPONSABILIDADES DO ÓRGÃO GERENCIADOR DA ATA DE REGISTRO DE PREÇOS (IN 94/2022SGD/ME – Art. 17, inciso III, alíneas "a" a "d")**

6.22.1. efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

6.22.2. conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

6.22.3. definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

a) as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou

b) sistema informatizado, quando disponível; e

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

6.22.5. definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

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

6.22.7. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda,

quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pela contratada; e

6.22.8. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no item 6.22.4, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

7. MODELO DE EXECUÇÃO E GESTÃO DO CONTRATO (IN 94/2022 SGD/ME – ART. 18 E 19)

7.1. DOS PRAZOS, HORÁRIOS DE FORNECIMENTO DE BENS, PRESTAÇÃO DOS SERVIÇOS E LOCAIS DE ENTREGA (IN 94/2022 SGD/ME – Art. 18, inciso I, alínea a)

7.1.1. Após a abertura da Ordem de Serviço, os bens que compõem a solução devem ser entregues em até 60 (sessenta) dias corridos.

7.1.2. Os equipamentos deverão ser entregues nas dependências do **HC-UFGM/Ebserh**, no horário compreendido entre 08h às 16h (horário de Brasília), de segunda a sexta-feira (dias úteis), no endereço:

Unidade de Patrimônio

Hospital das Clínicas da Universidade de Minas Gerais

Endereço: Avenida Alfredo Balena, 110

Santa Efigênia - Belo Horizonte - MG

CEP: 30.130-100

Telefone: (31) 3307-9390

7.1.3. De comum acordo, poderão ser combinados diferente horários e local de entrega.

7.1.4. A entrega dos equipamentos pela transportadora deverá ser previamente comunicada ao HC-UFGM/Ebserh com no mínimo 2 (dois) dias úteis de antecedência.

7.1.5. Os horários de execução dos serviços de instalação, configuração e migração deverão ser previstos no Plano de Projeto.

7.1.6. Após a entrega de todos itens que compõem a solução de segurança, será emitido em até 5 dias úteis o Termo de Recebimento Provisório **ANEXO III - (MODELO DO TERMO DE RECEBIMENTO PROVISÓRIO)**.

7.1.7. As etapas de execução do contrato deverão ocorrer conforme cronograma da tabela 01– cronograma de execução do contrato.

Tabela 01 – cronograma de execução do contrato

#	EVENTO	PRAZO	PREVISÃO DE EXECUÇÃO
1	Emitir a Ordem de Serviço	Dia D (de acordo com o interesse da contratante)	D0
2	Elaborar o plano de projeto	Até 20 (vinte) dias úteis após o evento #1	D+20
3	Realizar a entrega dos equipamentos	Até 60 (sessenta) dias corridos após o evento #1	D+60
4	Emissão do Termo de Recebimento Provisório (TRP)	Até 5 (cinco) dias úteis, após a conclusão do evento #3	D+65

#	EVENTO	PRAZO	PREVISÃO DE EXECUÇÃO
5	Realizar a implantação da solução	Até 30 (trinta) dias corridos, após a conclusão dos eventos #2 e #3.	D+90
6	Realizar treinamento para repasse de conhecimento	Iniciado em até 5 (cinco) dias úteis, após a conclusão do evento #5	D+95
7	Emissão do Termo de Recebimento Definitivo (TRD)	Até 10 (dez) dias úteis, após a conclusão do evento #5 e #6.	D+105
8	Emissão do Faturamento	Após o evento #7.	D+106
9	Ateste e Realização do Pagamento	Até 10 (dez) dias úteis, após o evento #8.	D+116

7.2. **DA DOCUMENTAÇÃO MÍNIMA EXIGIDA** (IN 94/2022 SGD/ME – Art. 18, inciso I, alínea b)

7.2.1. Deverá a CONTRATADA apresentar os relatórios de execução de serviço.

7.2.2. Deverá a CONTRATADA apresentar toda documentação referente ao fornecimento dos bens que compõem a solução.

7.2.3. Após conclusão da instalação a contratada deverá entregar o AS BUIT com o registro de todas as configurações realizadas.

7.3. **DOS PAPÉIS E RESPONSABILIDADES** (IN 94/2022 SGD/ME – Art. 18, inciso I, alínea c)

7.3.1. **Compete ao GESTOR DO CONTRATO:**

- I - Gerir e monitorar a execução do contrato;
- II - Orientar a fiscalização;
- III - Encaminhar ordens de serviço;
- IV - Tratar dos desvios de qualidade da prestação do serviço, quando necessário;
- V - Autorizar e encaminhar os faturamentos;
- VI - Assinatura do Termo de Recebimento Definitivo - TRD;
- VII - Encaminhamento de indicação de multas, glosas e sanções;
- VIII - Encaminhamento à Área Administrativa de eventuais pedidos de modificação contratual;
- IX - Manutenção do Histórico de Gestão do Contrato, contendo registros formais de todas as ocorrências positivas e negativas da execução do contrato;
- X - Apresentar, sempre que solicitado, informações gerenciais sobre a execução contratual.

7.3.2. **Compete ao FISCAL REQUISITANTE:**

- I - Avaliar a qualidade dos serviços realizados ou dos bens entregues e justificativas, a partir da aplicação das "Listas de Verificação" de acordo com os critérios de aceitação definidos em contrato;
- II - Identificação de não conformidade com os termos contratuais;
- III - Verificação da manutenção da necessidade, economicidade e oportunidade da contratação;
- IV - Confeção e assinatura do Termo de Recebimento Definitivo - TRD;
- V - Verificação da manutenção das condições definidas no Modelo de Gestão do contrato.

7.3.3. **Compete ao FISCAL TÉCNICO:**

- I - Avaliar a qualidade dos serviços realizados ou dos bens entregues e justificativas, a partir da aplicação das "Listas de Verificação" de acordo com os critérios de aceitação definidos em contrato;
- II - Identificação de não conformidade com os termos contratuais;
- III - Verificação da manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica;
- IV - Encaminhamento das demandas de correção à contratada;
- V - Apoio na verificação da manutenção da necessidade, economicidade e oportunidade da contratação;
- VI - Verificação da manutenção das condições definidas no Modelo de Execução do contrato;
- VII - Emitir ordens de serviço;
- VIII - Monitorar a execução do contrato;
- IX - Propor e implementar estratégias de controle e fiscalização;
- X - Apoiar o Gestor do Contrato quanto às questões técnicas contratuais;
- XI - Mediar conflitos na execução do contrato;
- XII - Solicitar a aplicações de sanções previstas, quando necessárias;
- XIII - Emitir o Termo de Recebimento Provisório - TRP;
- XIV - Registrar os chamados técnicos, acionar a garantia e acompanhar os acordos de níveis de serviços.

7.3.4. **Compete ao FISCAL ADMINISTRATIVO:**

- I - Acompanhar rotineiramente a execução dos serviços contratados, quanto aos aspectos administrativos, de forma a atuar tempestivamente na solução de eventuais problemas verificados;
- II - Encaminhar as questões que ultrapassam o âmbito das atribuições que lhe foram designadas aos respectivos responsáveis;
- III - Providenciar a obtenção de esclarecimentos, auxílio ou suporte técnico, para aqueles casos em que houver dúvida sobre a providência a ser adotada;
- IV - Zelar por uma adequada instrução processual, quanto à correta juntada de documentos;
- V - Verificação das regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento;
- VI - Aplicar as sanções administrativas;
- VII - Acompanhar o saldo de empenho;
- VIII - Formalizar o encerramento Contratual.

7.3.5. **Compete ao PREPOSTO:**

- I - Realizar a gestão das Ordens de Serviço e de outras demandas referentes à administração do CONTRATO;
- II - Acompanhar a execução das Ordens de Serviço;
- III - Assegurar-se de que as determinações da Ebserh sejam disseminadas e cumpridas pela CONTRATADA e com vistas à alocação dos recursos necessários para execução das Ordens de Serviço;

- IV - Informar sobre os problemas de qualquer natureza que possam impedir o bom andamento dos serviços;
- V - Elaborar documentos (relatórios gerenciais, relatórios de impacto) referentes ao acompanhamento da execução das Ordens de Serviço;
- VI - Executar os procedimentos administrativos referentes aos recursos alocados para execução dos serviços contratados;
- VII - Zelar pela qualidade dos serviços prestados;
- VIII - Exigir da equipe técnica da CONTRATADA o cumprimento de suas atribuições e adequação das atividades de acordo com as recomendações técnicas do fabricante, mormente quando estas, envolverem problemas e requisitos obrigatórios de segurança e compatibilidade.

7.4. DA QUANTIFICAÇÃO OU ESTIMATIVA PRÉVIA DO VOLUME DE SERVIÇOS DEMANDADOS, QUANTIDADE DE BENS A SEREM FORNECIDOS (IN 94/2022 SGD/ME – Art. 18, inciso II)

7.4.1. Deverão ser fornecidos os bens definidos neste termo de referência e seus anexos, conforme quantidades estabelecidas.

7.5. DA DEFINIÇÃO DE MECANISMOS FORMAIS DE COMUNICAÇÃO A SEREM UTILIZADOS PARA TROCA DE INFORMAÇÕES ENTRE A CONTRATADA E A EBSEH (IN 94/2022 SGD/ME – Art. 18, inciso III)

7.5.1. A solicitação de bens e serviços será por meio de emissão de Ordem de Serviço e Fornecimento de Bens **ANEXO IV - (MODELO DA ORDEM DE SERVIÇO)**.

7.5.2. Documentos formais deverão ser assinados, preferencialmente, pelo sistema SEI da Ebserh.

7.5.3. Deverão ser utilizados e-mails corporativos para envio de mensagens e documentos digitais.

7.5.4. Videoconferências, serão realizadas através de ferramenta institucional da Ebserh, preferencialmente o *Microsoft Teams*.

7.5.5. Os mecanismos de comunicação para fins de acionamento de garantia e suporte técnico deverão seguir as definições estabelecidas neste Termo de Referência.

7.6. DA FORMA DE PAGAMENTO (IN 94/2022 SGD/ME – Art. 18, inciso IV)

7.6.1. O pagamento será realizado em parcela única, por meio de Ordem Bancária.

8. DA GESTÃO E FISCALIZAÇÃO CONTRATUAL (IN 94/2022 SGD/ME – ART. 19)

8.1. Após a assinatura do Contrato, o HC-UFMG/Ebserh deverá nomear o Gestor do Contrato, o Fiscal Requisitante, o Fiscal Administrativo e o Fiscal Técnico.

8.2. A CONTRATADA deverá indicar formalmente o Preposto e um eventual substituto ao HC-UFMG/Ebserh.

8.3. O Preposto deverá estar disponível para contato e sempre que necessário, deverá ter disponibilidade para comparecer nas dependências do HC-UFMG/Ebserh.

8.4. A Gestão e a Fiscalização contratual deverão ser realizadas com base nos termos previstos no Contrato, no Termo de Referência e seus anexos.

8.5. O Gestor do Contrato e os Fiscais deverão promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais.

8.6. A fiscalização de que trata esta cláusula não exclui, nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade do HC-UFMG/Ebserh ou de seus agentes.

8.7. Os Fiscais, quando observarem qualquer situação técnica pertinente, que considerem irregular, deverão manifestar sua discordância junto ao preposto designado pela CONTRATADA e comunicar o Gestor do Contrato.

8.8. Todos os testes e relacionamentos entre os técnicos da CONTRATADA e a equipe do HC-UFMG/Ebserh devem ser efetuados no idioma português, sendo permitido interlocutor para tradução.

8.9. DAS ETAPAS PREVISTAS

8.9.1. Após a nomeação da equipe de Gestão/Fiscalização do contrato, a equipe do HC-UFMG/Ebserh deverá proceder-se com as atividades de início do contrato:

I - Elaboração do Plano de Inserção da CONTRATADA, pelo Gestor do Contrato e pelos Fiscais Técnico, Administrativo e Requisitante do Contrato, contemplando, no mínimo:

- a) o repasse à contratada de conhecimentos necessários à execução dos serviços ou ao fornecimento de bens;
- b) a disponibilização de infraestrutura à CONTRATADA, quando couber.

II - Elaboração do Plano de Fiscalização da CONTRATADA, pelo Gestor do Contrato e pelos Fiscais Técnico, Administrativo e Requisitante do Contrato, contemplando, no mínimo:

- a) o refinamento dos procedimentos de teste e inspeção detalhados no Modelo de Gestão do contrato, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo;
- b) configuração e/ou criação de ferramentas, computacionais ou não, para implantação e acompanhamento dos indicadores; e
- c) refinamento ou elaboração de Listas de Verificação e de roteiros de testes com base nos recursos disponíveis para aplicá-los.

III - Criação de processo administrativo específico, pela equipe de Gestão/Fiscalização do contrato, para registro histórico do contrato.

8.9.2. Após a assinatura do contrato, deverão ser observadas as etapas abaixo:

Tabela 2 – Principais etapas da execução contratual.

#	ETAPA	RESPONSÁVEL	PRAZO	ATIVIDADES
1 - REUNIÃO INICIAL				
1.1	Reunião Inicial	Gestor do Contrato Fiscal Técnico Fiscal Requisitante Fiscal Administrativo CONTRATADA	Após a assinatura do contrato.	1. Realização de reunião inicial convocada pelo Gestor do Contrato para o repasse à CONTRATADA de conhecimentos necessários à execução dos serviços ou ao fornecimento de bens, cuja pauta observará, pelo menos: a) presença do representante legal da contratada, que apresentará o preposto da mesma; b) entrega, por parte da contratada, do termo de Confidencialidade e do termo de Ciência; e c) esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.
2 - PROJETO, IMPLANTAÇÃO E TREINAMENTO				
2.1	Emitir a Ordem de	Gestor Contrato	Após a reunião inicial.	1 - Emitir a Ordem de Fornecimento de Bem - OFB

#	ETAPA	RESPONSÁVEL	PRAZO	ATIVIDADES
	Serviço			
2.2	Apresentar o Plano de Projeto	CONTRATADA	Até 20 (vinte) dias úteis, após a emissão da Ordem de Serviço	1. CONTRATADA deverá realizar visita(s) técnica(s) para averiguar condições de instalação para os equipamentos em cada local onde estes serão instalados, devendo: ○ verificar a infraestrutura física e lógica das dependências do HC-UFMG/Ebserh e demais pré-requisitos necessários à instalação dos equipamentos; ○ alinhar as condições de entrega e armazenamento dos equipamentos na unidade; ○ definir a estratégia de instalações dos equipamentos. 2. Emitir o Plano de Projeto para validação do HC-UFMG/Ebserh
2.3	Validar o Plano de Projeto	Gestor Contrato Fiscal Técnico Fiscal Requisitante	Até 5 (cinco) dias úteis após a emissão do Plano de Projeto	1. Validação do Plano de Projeto.
2.4	Realizar a entrega dos equipamentos	CONTRATADA	Em até 60 (sessenta) dias corridos a partir da abertura da Ordem de Serviço.	1. Entregar os equipamentos no local e prazo definido.
2.5	Sinalização de recebimento dos equipamentos	Fiscal Técnico	Até 5 (cinco) dias úteis após o recebimento da Entrega.	1. Validar os quantitativos de equipamentos entregues, conforme

#	ETAPA	RESPONSÁVEL	PRAZO	ATIVIDADES
				proposta e Nota Fiscal; 2. Emitir o Termo de Recebimento Provisório - TRP.
2.6	Realizar a instalação e configuração dos equipamentos	CONTRATADA	Até 30 (trinta) dias corridos após a emissão do TRP	1. Realizar os serviços de instalação, configuração e testes dos equipamentos. 2. Emitir a documentação final e completa do projeto
2.7	Realizar o repasse de conhecimento da Solução	CONTRATADA	Iniciado em até 5 (cinco) dias úteis após conclusão da implantação. Essa etapa pode ser remarcada a critério do HC-UFGMg/Ebserh, sem prejuízo às demais etapas.	1. Realizar o repasse de conhecimento sobre toda solução implantada. 2. Emitir certificado de participação.
2.8	Sinalização de conclusão da implantação da solução	CONTRATADA	Até 5 (cinco) dias úteis após conclusão da implantação plena da solução.	1. Emitir e disponibilizar a documentação final do projeto, completa e atualizada, de modo a sinalizar a conclusão da etapa de implantação 2. Solicitar a validação para fins de recebimento definitivo.
2.9	Emissão do Termo de Recebimento Definitivo	Fiscal Técnico Fiscal Requisitante Gestor do Contrato	Em até 10 (dez) dias úteis após o recebimento relatório de final do projeto.	1. Emitir o Termo de Recebimento Definitivo. 2. Emite autorização para Faturamento.
3 - DO FATURAMENTO				
3.1	Emissão das Notas Fiscais para Faturamento	CONTRATADA	Após a autorização de Faturamento.	1. Emissão da Nota Fiscal de faturamento contendo o detalhamento dos serviços executados, número de série dos equipamentos,

#	ETAPA	RESPONSÁVEL	PRAZO	ATIVIDADES
				quantidades e valores unitários e os materiais e serviços empregados, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pela CONTRATADA.
3.2	Realizar Pagamento	Fiscal Técnico Fiscal Administrativo Gestor do Contrato	Até 10 (dez) dias úteis após o recebimento da Nota Fiscal de Faturamento.	1. Elabora despacho de pagamento para o Unidade de Pagamento de Despesas; 2. Realiza a análise de certidões e conformidades, elabora despacho para Área Financeira; 3. Realiza o Pagamento. - o No caso do atraso de pagamento por conta da administração, sugere-se em caso de cobrança das multas e juros previstas em lei por este atraso, que está se dê por meio de cobrança separada do faturamento ordinário.

8.10. **DOS CRITÉRIOS DE ACEITAÇÃO DOS SERVIÇOS E BENS FORNECIDOS** (IN 94/2022 SGD/ME – Art. 19, inciso I)

8.10.1. **NA FASE DE HABILITAÇÃO:**

I - A licitante deverá anexar à Proposta de Preços **ANEXO V - (MODELO DA PROPOSTA DE PREÇOS)** a correlação entre os requisitos técnicos deste Termo de Referência e seus anexos, com os equipamentos e sistemas ofertados que compõem a solução de segurança, indicando a referência de cada item da especificação (ponto a ponto). A licitante que não apresentar a devida correlação terá sua proposta desclassificada.

8.10.2. **APÓS A IMPLANTAÇÃO DA SOLUÇÃO:**

I - Será realizado monitoramento da taxa de processamento do equipamento por um período de 24 horas para avaliar a performance durante os momentos de picos.

8.10.3. **APÓS A REALIZAÇÃO DO TREINAMENTO:**

I - O Setor de Tecnologia irá avaliar a capacitação, com pesquisa de satisfação e, caso a mesma não atinja pontuação superior a 80% (oitenta por cento), esta deverá ser reestruturada e aplicada novamente, sem nenhum custo adicional ao HC-UFMG/Ebserh.

8.11. **DOS PROCEDIMENTOS DE TESTE E INSPEÇÃO** (IN 94/2022 SGD/ME – Art. 19, inciso II)

8.11.1. O procedimento de comprovação do atendimento aos requisitos técnicos da solução de segurança, será realizado através da análise de documentos comprobatórios (*datasheets e ou* manuais), emitidos pelo fabricante do equipamento, disponibilizado pela proponente anexo ao ponto a ponto.

8.12. **DA FIXAÇÃO DOS VALORES E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO** (IN 94/2022 SGD/ME – Art. 19, inciso III)

8.12.1. Caso a CONTRATADA não atinja os valores mínimos aceitáveis fixados neste Termo de Referência, não venha a produzir os resultados esperados, deixe de executar as atividades contratadas, deixe de utilizar os materiais e recursos humanos exigidos para fornecimento da solução, ou utilize-os com qualidade ou quantidade inferior à demandada, estará sujeita a aplicação de glosas nos valores estabelecidos para multas e/ou penalidades ou retenção do pagamento até que as pendências sejam sanadas.

8.13. **DAS SANÇÕES ADMINISTRATIVAS APLICÁVEIS** (IN 94/2022 SGD/ME – Art. 19, inciso IV)

8.13.1. Esse tema será tratado no capítulo 09 desse TR.

8.14. **DOS PROCEDIMENTOS PARA O PAGAMENTO** (IN 94/2022 SGD/ME – Art. 19, inciso V)

8.14.1. O pagamento deverá ser precedido da conclusão dos serviços e entrega completa dos bens.

8.14.2. O pagamento será efetuado até o 20º (vigésimo) dia útil, a contar da emissão da nota fiscal de faturamento, que ocorrerá após a emissão do **Termo de Recebimento Definitivo**.

8.14.3. A CONTRATADA somente poderá emitir a nota fiscal de faturamento após autorização do Fiscal Técnico.

8.14.4. O valor faturado deverá ter descontado os valores oriundos da aplicação de eventuais glosas ou sanções, caso existam.

8.14.5. Constatando alguma incorreção nas notas fiscais que desaconselhe o seu pagamento, o prazo será contado a partir da respectiva regularização. O uso da carta de correção será admitida nos casos previstos pelas legislações tributárias.

8.14.6. A nota fiscal deverá ser emitida em favor do HC-UFMG/Ebserh, conforme endereço e CNPJ constante no Contrato.

8.14.7. Deverá ser indicado na nota fiscal o número do contrato, o mês de referência, a quantidade de cada item da solução, a descrição do item, o número de série do bem quando couber, o número do empenho, o valor unitário, o valor total, a referência à(s) Ordem de Serviço(s) ou a Ordem de Fornecimento de Bem, o nome do banco, a agência e número da conta corrente onde será efetuado o pagamento.

8.14.8. Os valores dos tributos incidentes sobre os serviços ora contratados deverão ser destacados na respectiva nota fiscal, sempre que a legislação tributária permitir, sendo certo que, no preço ajustado, já estarão inclusos os valores dos referidos tributos.

8.14.9. O atraso nos pagamentos devidos, motivados por descumprimento de obrigações da CONTRATADA, decorrentes de decisões relativas a multas ou outras sanções e seus recursos, não gera direito a reajustamento, correção ou quaisquer ônus adicionais para o HC-UFMG/Ebserh.

8.14.10. Os pagamentos efetuados à CONTRATADA não a isentarão de suas obrigações e responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade do serviço.

8.14.11. Os custos de eventuais erros de recolhimentos de impostos sob a responsabilidade do HC-UFMG/Ebserh, em decorrência de informações incorretas por parte da CONTRATADA, serão cobrados desta, que se obriga a ressarcir aquele no prazo de 5 (cinco) dias da notificação, sujeita às penalidades previstas no contrato.

8.14.12. A documentação de cobrança não aceita pelo HC-UFMG/Ebserh será devolvida à CONTRATADA para a devida correção, com as informações que motivaram sua rejeição pela fiscalização.

8.14.13. A devolução da documentação de cobrança, não aprovada pelo HC-UFGMg/Ebserh, não servirá de motivo para que a CONTRATADA suspenda a execução dos serviços.

8.14.14. O valor referente à multa será descontado de qualquer fatura ou crédito existente no HC-UFGMg/Ebserh em favor da CONTRATADA. Caso esse valor seja superior ao crédito eventualmente existente, a diferença será cobrada em fatura posterior ou administrativamente ou judicialmente, se necessário.

8.14.15. Em caso de eventual atraso do pagamento por culpa da própria administração pública, poderão ser adotados critérios de atualização monetária entre a data do adimplemento das obrigações e a data do efetivo pagamento.

8.15. DO ENCERRAMENTO CONTRATUAL

8.15.1. A CONTRATADA deverá garantir que a solução continue operacional, com todas as funcionalidades descritas neste Termo de Referência e anexos, habilitadas, mesmo após o encerramento da garantia. Sem obrigação de disponibilizar novas atualizações por parte do fabricante;

8.15.1.1. O HC-UFGMg/Ebserh deverá cancelar todos os perfis de acesso da CONTRATADA em seu ambiente computacional, providos durante a execução do contrato;

8.15.2. O HC-UFGMg/Ebserh deverá inativar as caixas postais da CONTRATADA, se aplicável;

8.15.3. O HC-UFGMg/Ebserh deverá realizar o encerramento administrativo do contrato, com a devida baixa de pendências de pagamentos e demais pendências em aberto;

8.15.4. O HC-UFGMg/Ebserh deverá emitir o Termo de Encerramento Contratual **ANEXO VI - (MODELO DO TERMO DE ENCERRAMENTO DO CONTRATO)**, que deverá ser assinado pelo representante legal da CONTRATADA.

9. DAS SANÇÕES ADMINISTRATIVAS APLICÁVEIS (IN 94/2022 SGD/ME – ART. 19, INCISO IV)

9.1. Pela inexecução total ou parcial do contrato a Ebserh poderá, garantido o regular processo administrativo, aplicar ao contratado as seguintes sanções:

I - Advertência;

II - Multa, na forma prevista no instrumento convocatório ou no contrato;

III - Suspensão temporária de participação em licitação e impedimento de contratar com a Ebserh, por prazo não superior a 2 (dois) anos.

9.2. Em caso de infração administrativa, a Administração pode aplicar à Contratada as seguintes sanções, nos termos do Regulamento de Licitações e Contratos da Ebserh:

9.2.1. Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para a Administração;

9.2.2. Multa:

I - conforme aplicação prevista no item 09.10;

II - compensatória de 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

III - em caso de outras hipóteses de inexecução parcial, poderá ser aplicada multa compensatória de até 20% (vinte por cento) do valor total do contrato, respeitados critérios de razoabilidade e proporcionalidade, considerando os impactos da obrigação inadimplida.

9.2.3. Suspensão de licitar e impedimento de contratar com a unidade contratante pelo prazo de até dois anos;

9.2.4. Suspensão de licitar e impedimento de contratar com o HC-UFGMg/Ebserh pelo prazo de até dois anos (abrangendo todas as unidades hospitalares vinculadas à Ebserh);

9.3. As sanções previstas nos subitens 09.2.1, 09.2.3 e 09.2.4 poderão ser aplicadas à Contratada juntamente com as de multa.

9.4. Eventuais multas aplicadas podem ser descontadas de pagamentos a serem efetuados.

9.5. Também ficam sujeitas às penalidades listadas as empresas ou profissionais que:

a) tenham sofrido condenação definitiva por praticar, por meio doloso, fraude fiscal no recolhimento de quaisquer tributos;

b) tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

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

9.6. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto no Regulamento de Licitações e Contratos da Ebserh.

9.7. 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.

9.8. As penalidades serão obrigatoriamente registradas no SICAF.

9.9. Não haverá aplicação de sanções decorrentes de inexecuções contratuais quando da ocorrência de caso fortuito ou força maior, devidamente comprovado pela CONTRATADA e acordado pelo HC-UFGM/Ebserh, de acordo com o disposto no *caput* e parágrafo único do art. 393 do Código Civil Brasileiro.

9.10. Em caso de ocorrências específicas, conforme a Lei 13.303/2016, sujeitar-se-á a CONTRATADA às seguintes sanções:

- a) Multa sobre o valor do contrato, conforme classificação abaixo:
 - I - **M1**: Multa de 5% (cinco por cento) sobre o valor do Contrato;
 - II - **M2**: Multa de 3% (três por cento) sobre o valor do Contrato;
 - III - **M3**: Multa de 1% (um por cento) sobre o valor do Contrato;
 - IV - **M4**: Multa de 0,5% (cinco décimos por cento) sobre o valor do Contrato;
 - V - **M5**: Multa de 0,3% (três décimos por cento) sobre o valor do Contrato;
 - VI - **M6**: Multa de 0,1% (um décimo por cento) sobre o valor do Contrato.

9.10.1. Quanto à entrega e/ou instalação dos equipamentos:

Tabela 03 – Sanções relacionadas à entrega e/ou instalação de equipamentos

ATRASO NA ENTREGA	PRAZO	SANÇÃO/MULTA
1ª Ocorrência	1º dia corrido após o prazo máximo de entrega estabelecido na tabela referente ao cronograma de execução do contrato	Notificação da Contratada
2ª Ocorrência	5º dia útil após a 1ª ocorrência.	Advertência
3ª Ocorrência	5º dia útil após a 2ª ocorrência.	Multa - M2
A partir da 4ª Ocorrência	5º dia útil após a 3ª ocorrência.	Multa - M1 / Abertura de processo administrativo para avaliação da execução Contratual, com possível rescisão do Contrato.

9.10.2. Quanto aos demais eventos:

Tabela 04 – Sanções relacionadas ao descumprimento contratual.

TIPO DE EVENTO	SANÇÃO	CLASSIFICAÇÃO	APLICAÇÃO	DESCRIÇÃO
Assinatura do contrato	MULTA	M3	POR EVENTO	Não realização da reunião inicial, com seus respectivos requisitos contratuais
Assinatura do contrato	MULTA	M3	POR EVENTO	Não assinatura do Termo de Confidencialidade e/ou

TIPO DE EVENTO	SANÇÃO	CLASSIFICAÇÃO	APLICAÇÃO	DESCRIÇÃO
				Termo de Ciência
Assinatura do contrato	MULTA	M3	POR EVENTO	Não realização da vistoria das instalações
Capacitação	MULTA	M3	POR EVENTO	Não realização do repasse de conhecimento conforme condições previstas
Fornecimento de equipamento	MULTA	M1	POR EVENTO	Fornecimento de equipamento usado ou remanufaturado ou fora de linha
Fornecimento de equipamento	MULTA	M4	POR DIA DE ATRASO	Não apresentação do Plano de Projeto no prazo previsto.
Fornecimento de equipamento	MULTA	M3	POR EVENTO	Falta de acessório ou material para a correta instalação dos equipamentos
Fornecimento de equipamento	MULTA	M4	POR DIA DE ATRASO	Não instalação e configuração da solução dentro do prazo
Fornecimento de equipamento	MULTA	M1	POR EVENTO	Equipamento não apresentar os requisitos mínimos
Fornecimento de equipamento	MULTA	M1	POR EVENTO	Não cumprimento com os requisitos do software de gerenciamento
Fornecimento de equipamento	MULTA	M3	POR EVENTO	Não comunicação quando da entrega ou retirada de produtos
Fornecimento de equipamento	MULTA	M5	POR DIA DE ATRASO	Não cumprimento do horário de entrega ou retirada de produtos
Gestão contratual	MULTA	M3	POR EVENTO	Profissional da contratada não demonstrar capacidade de atendimento técnico
Gestão contratual	MULTA	M2	POR EVENTO	Promover ação contrária ao disposto como deveres e responsabilidades da contratada
Gestão contratual	MULTA	M2	POR EVENTO	Não cumprimento das obrigações por parte dos técnicos ou gestor da contratada
Gestão contratual	MULTA	M3	POR EVENTO	Não comunicação à Ebserh de eventos de risco e problemas
Gestão contratual	MULTA	M3	POR EVENTO	Não fornecer a documentação solicitada

TIPO DE EVENTO	SANÇÃO	CLASSIFICAÇÃO	APLICAÇÃO	DESCRIÇÃO
				após a instalação da solução
Gestão contratual	MULTA	M4	POR DIA DE ATRASO	Não cumprir os prazos previstos para a solução de contorno, com severidade ALTA
Gestão contratual	MULTA	M5	POR DIA DE ATRASO	Não cumprir os prazos previstos para a solução de contorno, com severidade MÉDIA
Gestão contratual	MULTA	M6	POR DIA DE ATRASO	Não cumprir os prazos previstos para a solução de contorno, com severidade BAIXA
Gestão contratual	MULTA	M4	POR DIA DE ATRASO	Não cumprir os prazos previstos para reposição de componentes/equipamentos em garantia
Gestão contratual	MULTA	M2	POR EVENTO	Impossibilidade de abertura de chamado técnico
Gestão contratual	MULTA	M4	POR HORA DE ATRASO	NÍVEIS DE SERVIÇO - O não atendimento dentro do prazo estabelecido para o chamado de Severidade: 1 – Crítica
Gestão contratual	MULTA	M5	POR HORA DE ATRASO	NÍVEIS DE SERVIÇO - O não atendimento dentro do prazo estabelecido para o chamado de Severidade: 2 – Alta
Gestão contratual	MULTA	M6	POR HORA DE ATRASO	NÍVEIS DE SERVIÇO - O não atendimento dentro do prazo estabelecido para o chamado de Severidade: 3 – Média
Gestão contratual	MULTA	M6	POR HORA DE ATRASO	NÍVEIS DE SERVIÇO - O não atendimento dentro do prazo estabelecido para o chamado de Severidade: 1 – Baixa

9.10.3. A análise da equipe de fiscalização do contrato sobre as condições de incidência de multas deverão ocorrer em periodicidade mensal, caso o somatório das multas aplicadas atinja 10% (dez por cento) por mais de 2 (dois) meses consecutivos ou 4 (quatro) meses alternados dentro de 1(um) ano, proceder-se-á abertura de processo administrativo para avaliação do contrato, que poderá configurar a inexecução total do objeto.

10. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO (IN 94/2022 SGD/ME – ART. 20)

10.1. Em atenção ao art. 13 do Regulamento de Licitações e Contratos da Ebserh (art. 34, *caput*, da Lei 13.303, de 2016), a **estimativa de preços da contratação** será **sigilosa**.

10.2. O detalhamento da pesquisa de preços encontra-se no processo SEI nº (23537.014058/2024-63).

11. **DA ADEQUAÇÃO ORÇAMENTÁRIA E O CRONOGRAMA FÍSICO-FINANCEIRO (IN 94/2022 SGD/ME – ART. 21)**

11.1. As despesas decorrentes da contratação prevista neste Termo de Referência estão programadas em dotação orçamentária própria, prevista no Orçamento Geral da União para o exercício de 2024. Os valores estão registrados no Acordo Organizativo de Compromissos (AOC), processo SEI (23477.017796/2023-33), especificamente no grupo 5.

Tabela 05 – etapas do cronograma físico-financeiro.

#	EVENTO	PRAZO	PERCENTUAL PAGO
1	Emitir a Ordem de Serviço	Dia D após a assinatura do contrato	0% (zero)
2	Elaborar o plano de projeto	Até 20 (vinte) dias úteis após o evento #1	0% (zero)
3	Realizar a entrega dos equipamentos	Até 60 (sessenta) dias corridos após o evento #1	0% (zero)
4	Emissão do Termo de Recebimento Provisório (TRP)	Até 5 (cinco) dias úteis, após a conclusão do evento #3	0% (zero)
5	Realizar a implantação da solução	Até 30 (trinta) dias corridos, após a conclusão dos eventos #2 e #3.	0% (zero)
6	Realizar treinamento para repasse de conhecimento	Iniciado em até 5 (cinco) dias úteis, após a conclusão do evento #5	0% (zero)
7	Emissão do Termo de Recebimento Definitivo (TRD)	Até 10 (dez) dias úteis, após a conclusão do evento #5 e #6.	0% (zero)
8	Emissão do Faturamento	Após o evento #7.	0% (zero)
9	Ateste e Realização do Pagamento	Até 10 (dez) dias úteis, após o evento #8.	100% (cem por cento)

12. **DO REGIME DE EXECUÇÃO (IN 94/2022 SGD/ME – ART. 22)**

12.1. O Objeto deste contrato será executado sob o regime de contratação por preço unitário, em conformidade com o disposto no inciso XI, art. 5º, do Regulamento de Licitações e Contratos da Empresa Brasileira de Serviços Hospitalares.

13. DOS CRITÉRIOS TÉCNICOS PARA SELEÇÃO DO FORNECEDOR (IN 94/2022 SGD/ME – ART. 23)

13.1. As empresas, deverão comprovar, ainda, a qualificação técnica, por meio da comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação ou com os itens pertinentes, mediante a apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

13.2. A licitante vencedora deverá apresentar, juntamente com a proposta, atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando o fornecimento de um quantitativo mínimo de uma unidade de item similar ou superior ao licitado.

13.3. Os atestados devem conter nome (razão social), CNPJ e endereço completo do órgão emitente do atestado e licitante vencedora, características dos equipamentos, data de emissão, nome, cargo, telefone e assinatura do responsável pela emissão do atestado, em papel timbrado;

13.4. Os atestados solicitados visam garantir que as licitantes tenham condições de cumprir as obrigações objeto do contrato licitado, observando-se a comprovação da aptidão para o desempenho de atividade similar e compatível com o negócio praticado pela licitante vencedora.

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

13.6. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação de diferentes atestados.

13.7. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

13.8. A 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.

13.9. A licitante deverá indicar, claramente, quais itens do atestado apresentado, correspondem aos exigidos neste certame para habilitação técnica. Tal indicação pode ser realizada por relatório adicional que correlacione o atestado com os itens do Termo de Referência ou Contrato que originou o atestado de capacidade técnica apresentado.

13.10. O HC-UFMG/Ebserh poderá realizar diligências para averiguação da autenticidade dos atestados.

14. CRITÉRIOS GERAIS DE SELEÇÃO DE FORNECEDOR**14.1. Critério de julgamento:**

14.1.1. O critério de julgamento será o de menor preço unitário, nos termos do Regulamento de Licitações e Contratos da Ebserh - RLCE 2.0.

14.1.2. Em se tratando de grupo, o critério de julgamento desses itens deverá ser o de menor preço global.

14.2. Modo de disputa:

14.2.1. Será adotado para o envio de lances no pregão eletrônico o modo de disputa aberto.

14.3. Intervalo entre lances:

14.3.1. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser 0,20% (dois décimos por cento).

14.4. Condições de participação:

14.4.1. Para participação neste Pregão deverão ser observados:

a) as previsões constantes no art. 69 do [Regulamento de Licitações e Contratos da Ebserh](#) - RLCE 2.0, que define quais são as condições impeditivas de participar de licitações e de ser contratada pela Ebserh;

b) a Política de Transações com partes relacionadas da Ebserh atualizada que está disponível em <https://www.gov.br/ebserh/pt-br/governanca/governanca-corporativa/politica-de-transacoes-com-partes-relacionadas>;

- c) o atendimento por parte do licitante ao art. 7º, XXXIII da [Constituição da República Federativa do Brasil de 1988](#), que prevê "proibição de trabalho noturno, perigoso ou insalubre a menores de dezoito e de qualquer trabalho a menores de dezesesseis anos, salvo na condição de aprendiz, a partir de quatorze anos";
- d) a participação de interessados cujo ramo de atividade seja compatível com o objeto desta licitação e que estejam com Credenciamento regular no SICAF, conforme disposto no artigo 9º da [Instrução Normativa nº 03](#), de 2018;
- e) o previsto no art. 4º, inciso VI, do RLCE 2.0:

Art. 4º As seguintes diretrizes devem ser observadas nas contratações conduzidas pela Ebserh: (

...)

VI - observância de políticas de compras sustentáveis, de relacionamento com fornecedores, de integridade, de transação com partes relacionadas, de proteção de dados pessoais e outras políticas aprovadas no âmbito da Ebserh, que guardem pertinência com o objeto da contratação.

14.5. Condições de habilitação:

14.5.1. Deverão ser observados os requisitos de habilitação definidos no art. 65 do [Regulamento de Licitações e Contratos da Ebserh](#) - RLCE 2.0, bem como os definidos no Edital, tais como:

14.5.1.1. Habilitação jurídica:

14.5.1.1.1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

14.5.1.1.2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no [sítio www.portaldoempreendedor.gov.br](http://www.portaldoempreendedor.gov.br);

14.5.1.1.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

14.5.1.1.4. No caso de sucursal, filial ou agência: inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

14.5.1.1.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

14.5.1.1.6. No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764/1971;

14.5.1.1.7. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

14.5.1.1.8. Os documentos acima deverão estar acompanhados de todas as alterações relevantes ao objeto desta Licitação e à composição societária atual da empresa ou da última consolidação.

14.5.1.2. Regularidade fiscal e trabalhista:

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

14.5.1.2.2. Prova de inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

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

14.5.1.2.4. Prova de regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

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

14.5.1.3. Qualificação Econômico-Financeira:

14.5.1.3.1. Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante.

14.5.1.3.2. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais.

14.5.1.3.3. A aptidão econômica do licitante para cumprir as obrigações decorrentes desta contratação será verificada mediante a obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um) resultantes da aplicação das fórmulas:

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

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

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

14.5.1.3.4. As empresas que apresentarem resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar, considerados os riscos para a Ebserh, e a critério da autoridade competente, o patrimônio líquido ou capital social mínimo de 1% do valor da proposta apresentada para o item pertinente.

14.5.1.3.5. Exigência de patrimônio líquido ou capital social mínimo equivalente a 1% (um por cento) do valor da proposta apresentada pelo licitante.

Art. 65 § 13 e 14, inciso III, do RLCE 2.0

§ 13 Quando o requisito de informações sobre capacidade econômico-financeira estiver vinculado ao valor da contratação, o instrumento convocatório deverá indicar que a informação deverá se referir ao valor da proposta apresentada pelo licitante.

§ 14, inciso III O estabelecimento da exigência de capital mínimo ou de patrimônio líquido mínimo equivalente a até 10% (dez por cento) do valor da proposta apresentada pelo licitante, nas compras para entrega futura e na execução de obras e serviços.

14.5.1.3.6. O artigo 65, inc. IV, "a" do Regulamento de Licitações e Contratos da Empresa Brasileira de Serviços Hospitalares (RLCE 2.0), prescreve como documentos relativos à qualificação econômico-financeira:

IV - capacidade econômico-financeira, visando a demonstrar a aptidão econômica do licitante para cumprir as obrigações decorrentes do futuro contrato, devendo ser comprovada de forma objetiva, por coeficientes e índices econômicos previstos no edital, devidamente justificados no processo licitatório, e será restrita à apresentação da seguinte documentação:

a) balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais;

14.5.1.3.7. Os índices financeiros usualmente exigidos em certames licitatórios são os de liquidez geral, liquidez corrente e solvência geral, assim conceituados:

LIQUIDEZ GERAL: indica quanto a empresa possui em disponibilidades, bens e direitos realizáveis no curso do exercício seguinte para liquidar suas obrigações, com vencimento neste mesmo período.

LIQUIDEZ CORRENTE: indica quanto a empresa possui em recursos disponíveis, bens e direitos realizáveis a curto prazo, para fazer face ao total de suas dívidas de curto prazo.

SOLVÊNCIA GERAL: expressa o grau de garantia que a empresa dispõe em ativos (totais) para pagamento do total de suas dívidas. Envolve, além dos recursos líquidos, também os permanentes.

14.5.1.3.8. Para os três índices mencionados, o resultado "**>= 1**" (maior ou igual a um) é indispensável à comprovação da boa situação financeira, sendo que quanto maior o resultado melhor será a condição da empresa. Ademais, deve ser asseverado que caso as empresas não alcancem o resultado exigido nos índices (**>=1**), existe a possibilidade de comprovação do capital social ou patrimônio líquido de 10 % (dez por cento) do valor da contratação, que é admitido apenas de forma excepcional e justificada, nas compras para entrega futura (art. 65, §§ 13 e 14, inciso III, do RLCE 2.0), ampliando o universo de possíveis licitantes nos certames.

14.5.1.3.9. Portanto, a adoção dos índices não viola o caráter competitivo do certame, uma vez que não se vinculam à rentabilidade ou lucratividade dos licitantes, prestando-se tão somente à aferição da equilibrada situação financeira, constituindo-se em segurança para o Hospital das Clínicas da UFMG/Filial Ebserh na futura execução do contrato, sendo compatíveis com a complexidade exigida no objeto.

15. DO REAJUSTE DE PREÇOS (IN 94/2022 SGD/ME – ART. 24)

15.1. Os preços são fixos e irrevogáveis no prazo de um ano contado da data limite para a apresentação das propostas.

15.2. Dentro do prazo de vigência da contratação e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o Índice de Custos de Tecnologia da Informação - ICTI, instituído pela Portaria GM/MP nº 424, de 7 de dezembro de 2017, e mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

15.3. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

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

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

15.6. O reajuste será realizado por apostilamento.

16. DA NECESSIDADE DE REALIZAÇÃO DE PROVA DE CONCEITO (IN 94/2022 SGD/ME – ART. 12, § 1º)

16.1. Não haverá necessidade de realizar prova de conceito.

17. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO (IN 94/2022 SGD/ME – ART. 12, § 2º, INCISO I)

17.0.1. A Súmula nº 247/TCU dispõe que 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.

17.0.2. Por se tratar de processo de apenas um item, o parcelamento não se aplica para esse caso.

18. DA PARTICIPAÇÃO DE CONSÓRCIO E DA SUBCONTRATAÇÃO (IN 94/2022 SGD/ME – ART. 12, § 2º, INCISO II)

18.1. Face ao objeto de contratação, que prevê a "*Aquisição de equipamentos Firewall com recursos de próxima geração (NGFW), com Subscrição das Licenças de Segurança, suporte técnico e garantia por 60 meses, incluindo Serviço de Instalação e configuração*", a figura do consórcio não se justifica, dado que não há demanda que necessite de forças de trabalho diferentes ou dispersas para atendimento do objeto. Os potenciais fornecedores dos componentes previstos no objeto da contratação, tem plena condição de ofertar todos os itens previstos sem a necessidade de estabelecimento de Consórcio entre empresas. Durante o estudo foram consultados diversos certames da mesma natureza e notou-se como padrão a vedação da participação de consórcios o que demonstra ser prática de mercado.

18.2. Assim, o presente Termo de Referência não prevê as condições de participação de empresas reunidas em consórcio, vez que a experiência prática demonstra que as licitações que permitem essa participação são aquelas que envolvem serviços de grande vulto e/ou de alta complexidade técnica. Como o presente Termo foi elaborado com foco em práticas usuais e de amplo domínio do mercado fornecedor, consignou-se a vedação acima.

18.3. Destarte, caso fosse permitida a formação de consórcio, ao contrário do esperado, poderia ocorrer restrição à competição, caso dois ou mais fornecedores em potencial, viessem a formar consórcio para a participação no certame.

18.4. Não será permitida subcontratação total do objeto, a transferência ou a cessão das obrigações contratuais a terceiros.

18.5. Será permitido a subcontratação somente para a atividade de transferência de conhecimento desde que haja autorização expressa e por escrito da CONTRATANTE,

18.6. É vedado à CONTRATADA subcontratar atividades que envolvam o tratamento de dados pessoais sem autorização expressa e por escrito da CONTRATANTE.

18.7. Em caso de autorização da subcontratação, a CONTRATADA permanecerá totalmente responsável perante a CONTRATANTE pelo cumprimento das obrigações da empresa subcontratada, especialmente pelas obrigações de proteção dos dados pessoais.

19. **ENQUADRAMENTO DO OBJETO COMO BEM COMUM (IN 94/2022 SGD/ME – ART. 25, PARÁGRAFO ÚNICO)**

19.1. A natureza dos bens a serem contratados é comum, nos termos do inciso XIII, art. 6º, da Lei 14.133, de 2021;

XIII - bens e serviços comuns: aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado;

19.2. A prestação dos serviços relacionados às soluções não gera vínculo empregatício entre os empregados da CONTRATADA e a Ebserh, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta, assim não há o que se pensar em dedicação de mão de obra exclusiva.

19.3. Os materiais são classificados como de bem comum e são aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais do mercado.

19.4. Neste sentido, deve-se registrar que os requisitos de qualificação técnica e desempenho necessários para a prestação do serviço explicitado no Termo de Referência, foram objetivamente definidos por meio de especificações usuais praticadas no mercado e representa a real demanda do HC-UFMG/Ebserh, razão pela qual será adotado o critério de **MENOR PREÇO POR ITEM** para o julgamento objetivo das propostas.

20. **DA ALTERAÇÃO SUBJETIVA**

20.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que:

- I - Sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original;
- II - Sejam mantidas as demais cláusulas e condições do contrato;
- III - Não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da administração quanto a continuidade do contrato.

21. **DA VIGÊNCIA CONTRATUAL**

21.1. O prazo de vigência do contrato será de 60 (sessenta) meses, contado a partir da data de sua assinatura, posto que a assistência técnica poderá ocorrer ao longo do prazo da garantia contratual.

22. **DA GARANTIA CONTRATUAL**

22.1. A CONTRATADA fica obrigada a prestar garantia contratual no valor correspondente a 2,0% (dois por cento) do valor total do Contrato, em uma das modalidades previstas no art. 70, §1º, da Lei 13.303/2016:

- I - Caução em Dinheiro ou Título da Dívida Pública;
- II - Seguro Garantia;
- III - Fiança Bancária.

22.2. O documento original, ou cópia autenticada deste, referente à garantia contratual, deverá ser entregue à Ebserh, em até 10 (dez) dias úteis após o início de vigência do contrato;

22.3. Para a prestação da garantia contratual, fica vedado à CONTRATADA, pactuar com terceiros (seguradoras, instituições financeiras etc.) cláusulas de não ressarcimento ou não liberação do valor dado à garantia para o pagamento de multas por descumprimento contratual;

- 22.4. A Ebserh poderá utilizar o valor da garantia prestada para descontar os valores referentes a eventuais multas aplicadas à CONTRATADA, e satisfação de prejuízos causados à Ebserh ou a terceiros, na execução do objeto contratual por culpa ou dolo da CONTRATADA;
- 22.5. No período de vigência do contrato, a CONTRATADA deverá repor, no prazo de 15 (quinze) dias úteis, o valor da garantia eventualmente utilizado pela Ebserh;
- 22.6. Sobre a Liberação ou Restituição da Garantia Contratual:
- I - Ao fim da vigência do contrato, conforme especificado neste Termo de Referência, a CONTRATADA deverá realizar a solicitação formal da devolução da garantia contratual prestada.
 - II - A garantia prestada pela CONTRATADA somente será liberada ou restituída, atualizada monetariamente quando em dinheiro, após a execução do Contrato e o integral cumprimento de todas as cláusulas pactuadas, inclusive recolhimento de multas e satisfação de prejuízos causados a Ebserh ou a terceiros, na execução do objeto contratual por culpa ou dolo da CONTRATADA e mediante a emissão do documento formal de fiscalização final do contrato.

23. **DA ADESÃO À ATA DE REGISTRO DE PREÇOS (IN 94/2022 SGD/ME – ART. 15, INCISO V)**

A adesão à ata de registro de preços decorrente desta licitação será admitida apenas para as unidades hospitalares da Rede EBSEH e será realizada conforme recomendações do [Regulamento de Licitações e Contratos da Ebserh - RLCE](#).

24. **LISTA DE ANEXOS**

24.1. São partes integrantes deste Termo de Referência os respectivos anexos:

- I - ANEXO I do TR - MODELO DO TERMO DE CONFIDENCIALIDADE (39049636)
- II - ANEXO II do TR - MODELO DO TERMO DE CIÊNCIA (39049996)
- III - ANEXO III do TR - MODELO DO TERMO DE RECEBIMENTO PROVISÓRIO (39091379)
- IV - ANEXO VI do TR - MODELO DA ORDEM DE SERVIÇO (39095287)
- V - ANEXO V do TR - MODELO DA PROPOSTA DE PREÇOS (39124736)
- VI - ANEXO VI do TR - MODELO DE ENCERRAMENTO DO CONTRATO (39126447)
- VII - ANEXO VII do TR - MODELO DO TERMO DE RECEBIMENTO DEFINITIVO (39132996)
- VIII - ANEXO VIII do TR - PLANILHA PONTO A PONTO DE CUMPRIMENTO DE REQUISITOS DO TR (40516246)
- IX - ANEXOS DO TR - TODOS OS ANEXOS DO TR (40516292)

25. **DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO**

25.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria - SEI nº 051, de 11 de janeiro de 2024 (35803044).

25.2. Conforme o §6º do art. 12 da IN SGD/ME nº 94, de 2022, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

Integrante Requisitante

AGUINALDO DE MATOS FONSECA

SIAPE 225****

Chefe de Setor de Tecnologia da Informação e Saúde Digital

Integrante Técnico

ADRIANO FONSECA DE OLIVEIRA

SIAPE 235****

Analista de TI

Unidade de Infraestrutura Segurança e Suporte de Tecnologia da Informação

Integrante Administrativo

GISELE FERREIRA PINTO SIQUEIRA PEREIRA

SIAPE: 114****

Chefe da Unidade de Planejamento de Compras

Unidade de Planejamento de Compras

Em atendimento ao Parágrafo 3º do Art. 11 da IN 94/2022 da SGD/MP, este documento será assinado pela autoridade máxima do órgão, considerando que a autoridade máxima de TIC faz parte da Equipe de Planejamento da Contratação.

Autoridade máxima do órgão

ALEXANDRE RODRIGUES FERREIRA

SIAPE 124****

Superintendente

Superintendência



Documento assinado eletronicamente por **Aguinaldo de Matos Fonseca, Chefe de Setor**, em 10/07/2024, às 12:35, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Adriano Fonseca de Oliveira, Analista de Tecnologia da Informação**, em 10/07/2024, às 13:19, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Elizete Maria da Silva Neme, Superintendente, Substituto(a)**, em 10/07/2024, às 17:26, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Gisele Ferreira Pinto Siqueira Pereira, Chefe de Unidade**, em 29/07/2024, às 08:49, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.ebserh.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **40516453** e o código CRC **55AC4683**.

Referência: Processo nº 23537.000095/2024-94 SEI nº 40516453