



HOSPITAL UNIVERSITÁRIO LAURO WANDERLEY DA UNIVERSIDADE FEDERAL DA PARAÍBA
Rua Estanislau Eloy, s/nº - Bairro Castelo Branco
João Pessoa-PB, CEP 58050-585
- <http://hulw-ufpb.ebserh.gov.br>

Termo de Referência - TI - SEI

TERMO DE REFERÊNCIA

Referência: Arts. 12 a 24 IN SGD/ME Nº 1/2019

1. OBJETO DA CONTRATAÇÃO

Aquisição de **Solução Appliance Firewall, incluindo Instalação, Configuração e Treinamento** com alta disponibilidade para o Hospital Universitário Lauro Wanderley - Universidade Federal da Paraíba.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. Bens e serviços que compõem a solução

Grupo 01				
Id.	Descrição do Bem ou Serviço	Código CATMAT/CATSER	Quantidade	Métrica ou Unidade
01	A solução deve estar devidamente licenciada por 60 Meses para atender as funções e funcionalidades de no mínimo; Deve possuir Throughput de Firewall de no mínimo, 1Gbps; Deve possuir Throughput Threat de no mínimo, 1Gbps, com funcionalidades habilitadas simultaneamente devidamente atuantes: controle de aplicação, IPS e firewall. Os parâmetros de throughput consideram tráfego misto; Deve suportar, no mínimo, 300.000 sessões concorrentes; Deve possuir, no mínimo, 02 interfaces 10Gbps SFP+ e 08 interfaces 1Gbps RJ45; Devem ser fornecidos 04 módulos GBIC SFP+ 10Gbase-SR compatíveis para conexão no switch HPE 5900AF-48XG-4QSFP+ acompanhados de cordões ópticos. Incluindo os serviços de Instalação, configuração, migração da solução e treinamento para repasse de conhecimento.	481646	02	Unidade

2.1.1. A pesquisa de preço foi realizada pelo SETISD, observando o que determina a Norma Operacional nº 02/2019/DAI-EBSEH;

2.1.2. Em caso de divergência entre o descritivo do código CATMAT/CATSER e da “Descrição” contidos na tabela do item 2.1, prevalecerá o último;

2.2. **Da Justificativa do quantitativo**

2.2.1. O **item 1** destina-se a aquisição de 02 (dois) appliance de firewall novos para a disponibilização de alta disponibilidade ao HULW-UFPA, assim, alinhado a continuidade do negócio.

2.2.2. Considerando que o sistema de firewall roda em servidor obsoleto e fora de garantia; e pensando em agregar mais robustez à infraestrutura de TI a fim de atender à crescente necessidade de disponibilidade dos serviços de TIC.

2.2.3. Considerando que o HULW-UFPA atualmente não possui nenhum appliance de Firewall físico.

2.2.4. Considerando que, o que hoje existe de serviço de Firewall é uma VM executando o **PFSense na Versão 2.6.0**.

2.2.5. Considerando que é necessário que o item 01 tenha garantia e licenças por 60 (sessenta) meses, seguindo o que é especificado no item 6.1.7, letra "c", item 1 do Guia de boas práticas em contratação de soluções de tecnologia da informação elaborado pelo TCU (1). O tempo de 60 (Sessenta) meses justifica-se pela análise da semelhança da aquisição de computadores, situação em que se considera que o parque tecnológico seja totalmente renovado a cada ciclo de 4 (quatro) anos, permitindo preços mais competitivo em relação a aquisição de garantias e licenças de 36 (trinta e seis) meses.

3. **JUSTIFICATIVA PARA A CONTRATAÇÃO**

3.1. **Contextualização e Justificativa da Contratação**

3.1.1. O Hospital Universitário Lauro Wanderley (HULW-UFPA) possui diversos processos de trabalho informatizados, entre eles, a tramitação de processos administrativos internos, através da ferramenta SEI, a realização de registros médicos e assistenciais através da ferramenta AGHUX, atividades educacionais realizadas nas dependências da instituição, realização de videoconferências e reuniões diretamente relacionadas com o trabalho que é desenvolvido dentro da instituição.

3.1.2. 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, entre outros.

3.1.3. 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.

3.1.4. Uma das maneiras de se garantir 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.

3.1.5. 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 poder-se monitorar e analisar todo o tráfego de rede, garantindo maior segurança às informações institucionais.

3.1.6. 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.

3.1.7. O HULW-UFPA implanta e gerencia serviços e recursos de tecnologia da informação e comunicação através do Setor de Tecnologia da Informação e Saúde Digital (SETISD).

3.1.8. 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 TI.

3.1.9. 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.

3.1.10. 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) prevêem 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.

3.1.11. Pesquisas do Gartner apontam que 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.

3.1.12. 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 tais dados que atualmente já é realizado no ambiente do HULW-UFPB.

3.1.13. Logo, percebe-se o enorme desafio que se tem com a implantação da LGPD, principalmente para uma instituição hospitalar, nesse ínterim, faz-se necessário o uso de mecanismos que auxiliem na consecução de segurança, sigilo e boas práticas de governança junto ao tratamento de dados pessoais.

3.1.14. 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. Objetivos da contratação:

3.1.14.1. 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;

3.1.14.2. 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.

3.1.14.3. 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;

3.1.14.4. 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);

3.1.14.5. Melhorar o nível de qualidade e segurança dos serviços das aplicações internas da instituição;

3.1.14.6. 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).

3.2. **Da composição da solução a ser contratada**

3.2.1. Os itens aqui listados tem por objetivo garantir a manutenção dos serviços do Setor de Gestão de Tecnologia da Informação e Saúde Digital (SETISD). Estes itens fazem parte da solução de proteção de rede, que é composta por:

3.2.2. Dois appliance 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;

3.2.2.1. Um serviço de instalação e configuração, ativação de licenças e migrações de regras do firewall existente (PA 3220) nas dependências da instituição;

3.2.2.2. Um treinamento para 4 pessoas para utilização da solução de proteção de rede;

3.3. **Alinhamento aos Instrumentos de Planejamento Institucionais**

ALINHAMENTO AOS PLANOS ESTRATÉGICOS

Origem	Objetivos Estratégicos
Mapa Estratégico da Rede Ebserh 2018 - 2023	Gerir com competência, agilidade e transparência, garantindo continuidade das atividades na Rede.
Contrato Especial de Gestão EBSERH/HULW	Prover sistemas e infraestrutura de tecnologia da informação para o Hospital Universitário.

ALINHAMENTO AO PDTIC <2016-2019>

ID	Ação do PDTIC	ID	Meta do PDTIC associada
NE18	Contratação de renovação de licença e expansão de solução de firewall	NE18	Aquisição concluída

3.4. Estimativa da demanda

3.4.1. Demanda atendida no item 2.2

3.5. Parcelamento da Solução de TIC

3.5.1. Para julgamento e classificação das propostas será(ão) adotado(s) o(s) critério(s) de **TIPO MENOR PREÇO POR ITEM**, observadas as especificações constantes neste Termo de Referência;

3.5.2. Quanto à utilização da modalidade Registro de Preços, o objeto em questão se enquadra na hipótese II do art. 3º do Decreto nº. 11462/22, visto que em se tratando de bens ou serviços a serem adquiridos/contratados de forma parcelada, e não necessariamente de forma imediata, onde o fornecedor disponibiliza os bens e serviços a preços e prazos registrados em Ata específica e que, a aquisição ou contratação 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;

3.5.3. A natureza dos bens a serem contratados é comum, nos termos do art. 1º, parágrafo único, da Lei 14,.133/21;

3.6. Resultados e Benefícios a Serem Alcançados

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

3.6.2. Melhor aproveitamento de tempo e desempenho da equipe de TI da instituição, através de uma ferramenta de gerência facilitada;

3.6.3. Maior aderência às legislações vigentes, principalmente à LGPD, ao Marco Civil da Internet (lei nº 12.965/2014) e à Estratégia de Governo Digital (Decreto nº 10.332/2020), bem como maior facilidade da aplicação de tais comandos legais;

3.6.4. 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. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. 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;

4.1.2. 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);

4.1.3. Melhorar o nível de qualidade e segurança dos serviços das aplicações internas da instituição;

4.1.4. 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).

4.2. Requisitos de Capacitação

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

4.2.2. Cada 1 (uma) unidade deste serviço permite a capacitação de até 4 (quatro) pessoas no formato de turma;

4.2.3. O treinamento para a equipe de tecnologia da informação deverá ser realizado através de videoconferência ou presencial, em conjunto com a disponibilização de material digital como apostilas, manuais ou material áudio-visual dispondo sobre os procedimentos para a devida implantação da ferramenta, suas melhores práticas e esclarecimento de dúvidas;

4.2.4. A contratada deve apresentar cronograma da capacitação técnica e caso a contratante não concorde com as datas e horários propostos pela contratada, o cronograma deverá ser planejado em comum acordo entre as partes;

4.2.5. A capacitação técnica deve ser realizada nas dependências da contratante, ou através de vídeoconferência, com carga horária mínima de 20 horas, em data e horário a ser definido entre as partes;

4.2.6. A contratada deverá fornecer manual da solução em mídia eletrônica;

4.2.7. Deverá ser incluso no programa de treinamento o material didático equivalente ao oficial da fabricante da solução;

4.2.8. O treinamento deve oferecer em seu escopo:

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

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

4.2.8.3. 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.

4.2.8.4. O treinamento deverá contemplar no mínimo o conteúdo abaixo:

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

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

4.2.8.7. Criação e verificação de regras de firewall;

4.2.8.8. Criação e verificação de políticas de NAT;

4.2.8.9. Descriptografia;

4.2.8.10. Sandboxing de ameaças avançadas;

4.2.8.11. Integração de autenticação com Active Directory;

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

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

4.2.8.14. Configuração de VPN site-to-site;

4.2.8.15. Configuração de VPN client-to-site;

4.2.8.16. Configuração de VPN SSL;

4.2.8.17. Backup e restore de configuração;

4.2.8.18. Disaster recovery;

- 4.2.8.19. Atualização de firmware;
- 4.2.8.20. Monitoramento, criação e customização de relatórios;
- 4.2.8.21. Após o término dos serviços a contratada deverá fornecer certificados da capacitação técnica realizada;
- 4.2.9. Conteúdo programático:
 - 4.2.9.1. Arquitetura de funcionamento dos produtos;
 - 4.2.9.2. Configuração das funcionalidades suportadas pela solução;
 - 4.2.9.3. Configuração de gerenciamento.
- 4.2.10. A contratada disponibilizará à contratante o Certificado da execução da capacitação técnica com os seguintes dados:
 - 4.2.10.1. Nome do participante;
 - 4.2.10.2. Conteúdo da capacitação;
 - 4.2.10.3. Data;
 - 4.2.10.4. Carga horária;
 - 4.2.10.5. Frequência.
- 4.3. **Requisitos Legais**
 - 4.3.1. Constituição da República Federativa do Brasil de 1988;
 - 4.3.2. Lei nº 12.550/2011 - Autoriza o Poder Executivo a criar a empresa pública denominada Empresa Brasileira de Serviços Hospitalares - EBSERH; acrescenta dispositivos ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências;
 - 4.3.3. Decreto nº 8945/2016 - Regulamenta, no âmbito da União, a Lei nº 13.303, de 30 de junho de 2016, que 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 ;
 - 4.3.4. Lei nº 13.303/2016 - 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;
 - 4.3.5. Regulamento de Licitações e Contratos da EBSERH 2.0 (RLCE);
 - 4.3.6. Lei nº14.133/21 - Lei de licitações e contratos;
 - 4.3.7. Decreto nº 11.462/22 - Regulamenta os art. 82 a art. 86 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional.;
 - 4.3.8. Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
 - 4.3.9. IN SGD-ME nº 94/2022 - 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;
 - 4.3.10. Plano Diretor de Tecnologia da Informação 2023-2024 do Hospital Universitário Lauro Wanderley (HULW-UFPB).
- 4.4. **Requisitos de Manutenção**
 - 4.4.1. Entende-se como manutenção as atividades relativas ao bom funcionamento da solução que abrangem: garantia de funcionamento, suporte técnico e atualização da solução;
 - 4.4.2. A contratada deverá prestar garantia de funcionamento, suporte técnico e atualização por 60 (sessenta) meses, contados da data do aceite definitivo da instalação, configuração e ativação da solução. É de responsabilidade da contratada garantir que o suporte padrão por 60 (sessenta) 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;

4.4.3. 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);

4.4.4. O suporte técnico será acionado:

4.4.4.1. junto ao fabricante da solução de proteção de rede;

4.4.4.2. através de autorizada oficial do fabricante em território nacional; e

4.4.4.3. Junto ao contratado. Serão disponibilizados, no mínimo, os seguintes meios de abertura de chamados de suporte técnico:

4.4.4.3.1. página web;

4.4.4.3.2. e-mail; e

4.4.4.3.3. contato telefônico, por meio de ligações gratuitas, como através do sistema 0800;

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

4.4.5.1. **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;

4.4.5.2. **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;

4.4.5.3. **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;

4.4.5.4. **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;

4.4.6. 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;

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

4.4.8. 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);

4.4.9. Validação final do funcionamento normal do ambiente de produção, além de eventuais correções, quando necessário;

4.4.10. 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 30 (trinta) dias após o seu início, exceto por conveniência do contratante;

4.4.11. 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;

4.4.12. 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;

4.4.13. 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.

4.5. **Requisitos Temporais**

4.5.1. A Entrega dos equipamentos deverá ser efetivada no prazo máximo de 30 dias corridos a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela CONTRATANTE, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pela CONTRATADA e autorizado pela CONTRATANTE.

4.5.2. O contratado deverá entregar os bens e serviços que compõem a solução de proteção de rede nos prazos definidos, além do devido cumprimento dos diversos prazos relacionados aos processos de instalação e requisitos administrativos presentes neste termo de referência.

4.6. **Requisitos de Segurança**

4.6.1. 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;

4.6.2. 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.

4.6.3. Promover o afastamento em relação ao objeto da contratação, no prazo máximo de 24 (vinte e quatro) horas após o recebimento da notificação, de qualquer dos seus recursos técnicos que não correspondam aos critérios de confiança ou que perturbe a ação da equipe de fiscalização da CONTRATANTE.

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

4.7.1. Durante a prestação dos serviços contratados, os funcionários da empresa contratada deverão observar, no trato com os empregados e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público.

4.7.2. Os equipamentos devem estar aderente à Lei nº 12.305, de 2 de agosto de 2010, que Institui a Política Nacional de Resíduos Sólidos.

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

4.8. **Requisitos de Arquitetura Tecnológica**

4.8.1. Permitir autenticação centralizada tanto da rede cabeada como da rede sem fio utilizando-se da base AD existente (também deve suportar base LDAP);

4.8.2. Permitir que os logs de acesso dos usuários sejam armazenados pelo período mínimo de 01 ano, permitindo adequação com o Marco Civil da Internet;

4.8.3. Permitir a descentralização do tráfego SSL e SSH para inspeção de conteúdo;

4.8.4. Permitir inspeção em camada 7 (nível de aplicação);

4.8.5. Permitir inspeção de conteúdo com capacidade de identificar e bloquear vulnerabilidades, vírus, malwares conhecidos e desconhecidos;

4.8.6. Permitir a criação de redes seguras (VPN) de forma simples para que os usuários e os administradores possam utilizar da infraestrutura da instituição remotamente;

4.8.7. Permitir alta disponibilidade;

4.8.8. Deve possuir throughput de, no mínimo, 6.7 (seis ponto sete) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;

4.8.9. Deve possuir throughput de, no mínimo, 3.1 (três ponto um) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução;

- 4.8.10. Deve suportar, no mínimo, 100.000 (cem mil) novas conexões por segundo;
- 4.8.11. Implementar solução de firewall com suporte e garantia no idioma português e com SLA de atendimento diferenciado para chamados críticos;
- 4.8.12. Implementar solução de mercado, a fim de facilitar a padronização de acordo com as melhores práticas existentes;
- 4.8.13. Proteção do ambiente de rede contra ameaças através da detecção e proteção em tempo real contra ameaças (IDS/IPS);
- 4.8.14. As funcionalidades de IPS, anti-vírus e anti-spyware devem operar em caráter permanente e deverão possuir assinatura válida durante todo o período de garantia para recebimento automático de atualização para as suas bases de proteção;
- 4.8.15. Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, entre outras;
- 4.8.16. Criação de políticas e medidas de segurança para proteção da rede contra tentativas de ataques e invasões;
- 4.8.17. Prover o acesso com maior segurança à rede corporativa;
- 4.8.18. Permitir a gerência de certificados digitais;
- 4.8.19. Disponibilizar as atualizações, suporte e garantia do equipamento durante a vigência contratual;
- 4.8.20. Garantir as funcionalidades de segurança da solução mesmo após o término da garantia;
- 4.8.21. Registrar todas as ocorrências de acesso à rede a fim de monitorar possíveis acessos indevidos;
- 4.8.22. O dimensionamento da solução deverá ser realizado considerando o cenário atual desta instituição. Contudo, a solução deve possibilitar o crescimento futuro da infraestrutura de links de internet, preservando o investimento já realizado;
- 4.8.23. Solução de segurança integrada, serviço de instalação e configuração da solução, e serviço de capacitação técnica;
- 4.8.24. A solução deve estar licenciada por 60 (sessenta) meses para atender as funcionalidades de: controle de aplicações, proteção IPS, proteção anti-vírus (navegação, e-mail, arquivos), web filtering, análise de malwares modernos em nuvem, balanceamento de links, VPN e gerenciamento de logs;
- 4.8.25. Deve possuir integração com Microsoft Active Directory (para os seguintes sistemas operacionais: Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 e/ou Windows Server 2022) para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 4.8.25.1. A solução de proteção de rede deverá possuir as seguintes características de firewall de próxima geração:
- 4.8.25.1.1. filtro de pacotes;
- 4.8.25.1.2. controle de aplicações, inclusive em camada 7 da topologia OSI/ISO;
- 4.8.25.1.3. controle de largura de banda e qualidade de serviço (QoS);
- 4.8.25.1.4. rede privada virtual (VPN IPSEC e VPN SSL);
- 4.8.25.1.5. serviço de prevenção de intrusão (IPS);
- 4.8.25.1.6. serviço de proteção contra vírus, spywares e malwares (inclusive zero day);
- 4.8.25.1.7. filtro de URL ou filtro web;
- 4.8.25.1.8. controle de transmissão de dados e acesso à internet.
- 4.8.26. O equipamento firewall que compõem a solução de proteção de rede de dados deverá ser composto por hardware e software de forma integrada, comumente conhecido como appliance, não sendo aceitos equipamentos de propósito genérico (PCs ou servidores);
- 4.8.27. A solução proposta deve ser compatível com a composição por mais de 01 (um) appliance, sendo tal composição totalmente integrada, geralmente conhecido pelo conceito de cluster, com intuito de garantir a alta disponibilidade/redundância

da solução de proteção de rede de dados;

- 4.8.28. Cada appliance deverá suportar, no mínimo 900 (novecentos) mil conexões concorrentes;
- 4.8.29. Conter, por appliance, fonte de alimentação elétrica interna capaz de operar entre 120 a 240 AC, por reconhecimento automático do nível de tensão, com no mínimo duas fontes redundantes e independentes e que, em ao menos uma delas, permita-se sua retirada e inserção com o equipamento em funcionamento ("a quente" ou hot-swappable);
- 4.8.30. A solução deverá possuir ao menos 04 (quatro) interfaces físicas de rede de 10 gbps no padrão SFP+, por appliance;
- 4.8.31. Conter, no mínimo quatro (4) interfaces físicas de rede de 1 GE no padrão SFP, por appliance;
- 4.8.32. Ter no mínimo quatro (4) interfaces físicas de rede de 1 GE no padrão RJ45, por appliance;
- 4.8.33. Deverá possuir ao menos uma (1) interface física de rede de 1 GE dedicada para gerenciamento, por appliance;
- 4.8.34. Possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 10 GE dedicadas para o recurso de alta disponibilidade e redundância, por appliance;
- 4.8.35. Deverá possuir ao menos uma (1) interface física da porta console ou similar, por appliance;
- 4.8.36. Deverá ser fornecido, junto com a solução, ao menos 4 (quatro) cabos de port AOC (active optical cable) ou DAC de 10 gbps no padrão SFP+ com no mínimo 5 (cinco) metros de comprimento cada cabo, compatível com a solução e com switches da marca Aruba 3810M-16 SFP (JL075A);
- 4.8.37. Devem ser fornecidos 4 módulos GBIC SFP+ 10gbase-SR compatíveis com a plataforma de segurança solicitada e com switches da marca Aruba 3810M-16 SFP (JL075A), por appliance;
- 4.8.38. Deverá possuir disco solid state drive (SSD) com espaço de armazenamento de, no mínimo, 240 GB, por appliance;
- 4.8.39. Todos os firmwares, ou qualquer outro software componente da solução devem estar na versão mais atualizada disponível;
- 4.8.40. Os equipamentos fornecidos deverão ser próprios para montagem em rack do tipo 19 polegadas, com tamanho máximo de 1U, incluindo conjunto do trilho para adaptação e cabos de alimentação elétrica, com todas as adaptações necessárias ao padrão brasileiro de tomadas, caso seja necessário;
- 4.8.41. O recurso de alta disponibilidade poderá atuar nos modos ativo/passivo ou ativo/ativo, com a sincronização dos seguintes itens:
- 4.8.41.1. sessões;
- 4.8.41.2. configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
- 4.8.41.3. certificados descryptografados; associações de segurança das VPNs; tabelas de roteamento;
- 4.8.42. A solução deverá possuir suporte ao recurso de VLAN (IEEE 802.1q), com no mínimo 4094 (quatro mil e noventa e quatro) VLANs;
- 4.8.43. Atuar como servidor DHCP e retransmissor (relay) DHCP e ter o recurso de DHCP cliente;
- 4.8.44. Ter suporte ao serviço de agregação de conexões pelo protocolo 802.3ad (LACP);
- 4.8.45. Possuir suporte ao serviço de NAT nas modalidades 1-to-1, Many-to-1, Many-to-Many, NAT de origem, NAT de destino, tradução de porta (PAT);
- 4.8.46. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico, assim como NAT64 e NAT46;
- 4.8.47. Suporte ao recurso do protocolo Link Layer Discovery Protocol (LLDP);
- 4.8.48. Ter compatibilidade com o recurso de rede virtual privada (VPN) dos tipos Site-to-Site e Client-to-Site, bem como VPNs do tipo SSL e IPSEC;

- 4.8.49. Quanto ao recurso de VPN SSL, a solução de proteção de rede possibilitará que o usuário se conecte através de cliente instalado no sistema operacional do usuário ou através de interface web, sendo possível a atribuição de endereços IPs fixos e/ou dinâmicos, atribuição de DNS e criação de rotas de acesso de forma customizada por usuário e grupos de usuário LDAP e AD nos usuários remotos conectados através de VPN SSL;
- 4.8.50. Ter o recurso de portal de autenticação prévia (captive portal), sem instalação de agente ou cliente de software, em dispositivos que solicitem acesso à internet;
- 4.8.51. Tanto os appliances como a gerência centralizada deverão suportar monitoramento através de SNMP;
- 4.8.52. Implementar mecanismo de sincronismo de horário através do protocolo NTP;
- 4.8.53. Deve oferecer as funcionalidades de backup/restore, assim como permitir ao administrador agendar procedimentos de backups da configuração em determinado dia e hora;
- 4.8.54. Deve possibilitar o envio de logs para serviços de monitoramento externos, com suporte no mínimo ao protocolo syslog, bem como o envio de forma segura através de protocolo SSL/TLS;
- 4.8.55. Deverá apresentar suporte a SD-WAN;
- 4.8.56. 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:
- 4.8.56.1. resumo criptográfico do endereço IP de origem;
 - 4.8.56.2. resumo criptográfico do endereço IP de origem e destino;
 - 4.8.56.3. pela técnica conhecida como round-robin;
 - 4.8.56.4. por peso ou prioridade;
 - 4.8.56.5. por políticas de usuários e grupos de usuários de serviços baseados no protocolo LDAP, como o Microsoft Active Directory;
 - 4.8.56.6. através de políticas de aplicação e porta de destino;
- 4.8.57. Suportar roteamento IPv4 de forma estática e dinâmica, pelos protocolos RIPv2, BGP e OSPFv2;
- 4.8.58. Deverá implementar o controle de políticas/regras por porta, protocolo, aplicações, grupos estáticos e grupos dinâmicos (com base em características e comportamento) de aplicações, por usuários e grupos de usuários de serviços baseados no protocolo LDAP/AD, endereços IPs ou redes de endereço IP e por país de origem ou destino do endereço IP;
- 4.8.59. Suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado(s) país(es) seja bloqueado;
- 4.8.60. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- 4.8.61. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;
- 4.8.62. Implementar o controle, inspeção, e descriptografia do padrão SSL e SSH nos tráfegos de entrada e saída;
- 4.8.63. 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;
- 4.8.64. A solução contará com a possibilidade de agendamento de políticas/regras em horários pré-definidos, habilitando ou desabilitando tais políticas/regras;
- 4.8.65. A solução será capaz de reconhecer, e permitir liberação e bloqueio de aplicações, independente de portas ou protocolos de rede usados por tais aplicações, num montante mínimo de 1500 (mil e quinhentas) aplicações reconhecidas, tais como: redes sociais, compartilhamento de arquivos, email, atualizações de softwares, acesso remoto, voip, áudio e vídeo, peer-to-peer (p2p), proxy, messageiros instantâneos, etc (não é uma lista detalhada);
- 4.8.66. 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,

httptunnel, 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;

- 4.8.67. Deve permitir o bloqueio total de aplicações proxies (exemplo: Ultrasurf, GPass, FreeGate, Hopster, Tor, HotSpot Shield);
- 4.8.68. Suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
- 4.8.69. Identificar e bloquear comunicação com botnets;
- 4.8.70. Permitir a liberação e/ou bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- 4.8.71. Possuir módulo de IPS, anti-vírus e anti-spyware integrados na própria appliance de firewall;
- 4.8.72. Permitir o bloqueio de vulnerabilidades e de exploits conhecidos;
- 4.8.73. Incluir proteção contra ataques de negação de serviço (DoS);
- 4.8.74. Detectar e bloquear a origem de portscans, permitindo a criação de exceções para endereços IPs de ferramentas de monitoramento da instituição;
- 4.8.75. 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;
- 4.8.76. Permitir a visualização dos resultados das análises de malwares do tipo zero day nos diferentes sistemas operacionais suportados;
- 4.8.77. A solução deverá incluir proteção contra ataques de negação de serviços, impedir ataques básicos como Synflood, ICMPflood e UDPflood, detectar e bloquear a origem de portscans, identificar e bloquear comunicação com botnets e bloquear ataques realizados por worms conhecidos permitindo ao administrador acrescentar novos padrões de ataques worm;
- 4.8.78. Deverá possuir ferramenta de diagnóstico do tipo tcpdump;
- 4.8.79. Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica (HTTPS), quanto em CLI (linha de comando: SSH);
- 4.8.80. Deverá permitir autenticação de usuários em base local, servidor LDAP/AD, RADIUS e TACACS;
- 4.8.81. Deve permitir a criação de administradores independentes, para diferentes partes da solução de segurança, para que possa ser gerenciada por equipes distintas;
- 4.8.82. Deverá permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
- 4.8.83. Possibilitar a criação de assinaturas personalizadas de aplicações proprietárias na interface gráfica da solução, sem a necessidade de intervenção do fabricante;
- 4.8.84. Caso o reconhecimento de aplicações se dê também através do uso de base de assinaturas, a solução de proteção de rede terá de atualizar tal base de forma automática;
- 4.8.85. Deverá permitir a diferenciação e controle de partes das aplicações, como por exemplo, permitir uma aplicação de mensagem instantânea, mas não permitir na mesma aplicação a transferência de arquivos;
- 4.8.86. A solução de proteção de rede alertará o usuário quando uma aplicação for bloqueada;
- 4.8.87. A capacidade de detecção do usuário de rede integrada ao protocolo LDAP/AD, especificamente da solução Microsoft Active Directory, será feita sem a necessidade de implantação de agente da solução de proteção de rede no controlador de domínio e nas estações de trabalho dos usuários;
- 4.8.88. Deve suportar autenticação para smartphones e tablets;
- 4.8.89. A solução será capaz de análise de malwares não conhecidos, podendo ser tal análise local ou na "nuvem", onde será feita a execução e simulação do malware em ambiente controlado (sandbox);

- 4.8.90. 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;
- 4.8.91. O filtro de URL deverá possibilitar a criação de políticas/regras por categorização das URLs ou por URL específica, funcionando de forma transparente (proxy transparente) ou explícita;
- 4.8.92. O filtro de URL deverá possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;
- 4.8.93. O filtro de URL deverá também proteger contra o roubo de credenciais (usuários e senhas), identificadas através da integração com o Active Directory, submetidos em sites não corporativos, e permitir a criação de regra onde os usuários do Active Directory só possam enviar informações de login para sites autorizados na solução, além de bloquear o acesso de usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing;
- 4.8.94. Quanto ao recurso de filtro de URL, a solução deverá ser capaz de customizar a página de bloqueio exibida ao usuário;
- 4.8.95. Suporte à integração para identificação de usuários e grupos de usuários através dos protocolos LDAP/AD e RADIUS, bem como possibilitar a criação de grupos de usuários na solução de proteção de rede com base em atributos de tais protocolos;
- 4.8.96. A solução de proteção de rede contará com filtro de dados capaz de identificar e prevenir a transferência de arquivos mesmo dentro de aplicações, podendo tais arquivos serem identificados, no mínimo, por sua extensão/tipo e por sua assinatura;
- 4.8.97. A solução de proteção de rede terá garantido, durante todo período em que houver contratualização vigente, todas as atualizações de software e firmwares dos equipamentos que compõem a solução, disponibilizadas em data posterior ao da implantação da solução, permitindo manter a solução devidamente atualizada em sua última versão;
- 4.8.98. Funcionalidades como controle de aplicações, regras de firewall, VPN IPSec e VPN SSL, qualidade de serviço e modelagem de tráfego (QoS), decifração de tráfegos SSL e SSH, IPS, anti-vírus e anti-spyware devem funcionar de forma permanente, mesmo sem o direito de receber atualizações, ou que não haja contrato de garantia e suporte junto ao fabricante/fornecedor;
- 4.8.99. O gerenciamento da solução deve permitir, além de outras funcionalidades, as seguintes:
- 4.8.99.1. criar e administrar políticas de firewall e controle de aplicações;
- 4.8.99.2. criar e administrar políticas de IPS, anti-vírus e anti-spyware;
- 4.8.99.3. criar e administrar políticas de filtro web/URL;
- 4.8.99.4. monitorar e investigar registros de eventos (logs);
- 4.8.99.5. capturar pacotes;
- 4.8.99.6. pesquisar nos equipamentos da solução através de texto itens como: nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, e outros itens;
- 4.8.100. O gerenciamento da solução deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regras, e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve realizar também a 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;
- 4.8.101. O gerenciamento centralizado poderá ser entregue como appliance físico ou software. Caso seja entregue em appliance físico deve ser compatível com rack de 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em software deve ser homologado com ambientes VMware na versão ESXi 5.5 no mínimo, e/ou XCP-ng na versão 8.1 no mínimo, e/ou Microsoft Hyper-V 2019 ou superior;
- 4.8.102. Centralizar os logs e relatórios, usando uma única interface de gerenciamento;
- 4.8.103. O gerenciamento da solução deve suportar acesso, no mínimo, via SSH, cliente ou web (HTTPS);

- 4.8.104. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais windows ou linux;
- 4.8.105. Monitoração de logs e ferramentas de investigação de logs;
- 4.8.106. Captura de pacotes;
- 4.8.107. Deve permitir o acesso concorrente de administradores;
- 4.8.108. Deve permitir o bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;
- 4.8.109. Deve permitir visualizar quantidade de tráfego utilizado de aplicações e navegação;
- 4.8.110. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 4.8.111. Autenticação integrada ao Microsoft Active Directory (AD), LDAP, servidor radius ou base de dados local;
- 4.8.112. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração, para fins de auditoria;
- 4.8.113. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, anti-vírus e anti-spyware), URLs e filtro de arquivos, para melhor diagnóstico e resposta à incidentes;
- 4.8.114. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
- 4.8.115. Deve prover uma visualização sumarizada das aplicações e URLs que passaram pela solução;
- 4.8.116. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução;
- 4.8.117. Deve ser possível exportar os logs;
- 4.8.118. Exibição das seguintes informações, de forma histórica ou em tempo real:
- 4.8.118.1. Situação do dispositivo e do cluster;
- 4.8.118.2. Principais aplicações;
- 4.8.118.3. Principais ameaças;
- 4.8.118.4. Uso de CPU.
- 4.8.119. No mínimo os seguintes relatórios devem ser gerados:
- 4.8.119.1. Resumo gráfico de aplicações utilizadas;
- 4.8.119.2. Principais aplicações por utilização de largura de banda;
- 4.8.119.3. Principais aplicações por taxa de transferência de bytes;
- 4.8.119.4. Principais hosts por número de ameaças identificadas;
- 4.8.119.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, ameaças de rede vinculadas a este tráfego;
- 4.8.119.6. Deve permitir a criação de relatórios personalizados.
- 4.8.120. Gerar alertas automáticos via e-mail, SNMP e syslog;
- 4.8.121. O gerenciamento deve permitir/possuir no mínimo:
- 4.8.121.1. Criação e administração de políticas de firewall e controle de aplicação;
- 4.8.121.2. Criação e administração de políticas de IPS e anti-malware;
- 4.8.121.3. Criação e administração de políticas de filtro de URL;

- 4.8.121.4. Deve permitir usar palavras-chave e cores para facilitar identificação de regras;
- 4.8.121.5. Alerta de alterações, no caso acesso simultâneo de dois ou mais administradores;
- 4.8.121.6. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 4.8.121.7. Autenticação integrada ao Microsoft Active Directory (AD), LDAP e servidor radius;
- 4.8.121.8. Localização de em quais regras um endereço IP, faixa de IPs, sub-rede ou objetos estão sendo utilizados;
- 4.8.121.9. Deve suportar a programação de relatórios automáticos, para as informações básicas que precisa extrair diária, semanal e mensal. Backup das configurações e rollback de configuração para a última configuração salva;
- 4.8.121.10. Deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras.
- 4.8.122. O software de gerenciamento e relatórios deve ser entregue instalado, configurado, com os relatórios configurados e acessíveis.

4.9. **Requisitos de Projeto e de Implementação**

- 4.9.1. Não serão aceitas soluções ou funcionalidades implementadas via software ainda em fase de desenvolvimento, ou seja, aquelas que ainda não foram homologadas pelo fabricante para ambiente de produção;
- 4.9.2. A console WEB deve ser acessível por browsers que suportam a tecnologia HTML5;
- 4.9.3. A console WEB deve permitir integração com Active Directory da Microsoft para autenticação, ou então, utilizar autenticação local;
- 4.9.4. A solução deverá possuir ferramenta de checagem interna integrada a console de gerenciamento, buscando por problemas de saúde no cluster proativamente;
- 4.9.5. Deve ser constituído de equipamentos com tecnologia modular que permitam sua expansão sem interrupções dos serviços de rede e aplicações, com detecção automática de inclusão de novos appliance;
- 4.9.6. A ferramenta de gerenciamento deve fornecer um dashboard reportando a utilização dos recursos do cluster como CPU, Memória e Armazenamento;
- 4.9.7. A solução deve fornecer desempenho e disponibilidade adequados para as cargas de trabalho críticas da organização;
- 4.9.8. Solução deve incluir recursos de segurança adequados, como criptografia, autenticação, controle de acesso e monitoramento de atividades;

4.10. **Requisitos de Implantação**

- 4.10.1. As atividades de instalação deverão ser realizadas dentro do horário comercial.
- 4.10.2. A implantação deverá abranger a configuração de quaisquer funcionalidades suportadas pelo equipamento / software – desde que especificadas neste TR.
- 4.10.3. Estas informações serão documentadas no termo de abertura do projeto a ser documentado pela CONTRATADA após alinhamento do escopo de trabalho entre CONTRATADA e CONTRATANTE.
- 4.10.4. Todo o processo de instalação e configuração realizado deverá ser documentado pela CONTRATADA sob a forma de relatório.
- 4.10.5. A instalação física compreenderá a desembalagem e montagem de todos os componentes que integram a especificação dos dispositivos, a instalação física em ambiente interno ou externo, conexão à rede de dados e alimentação elétrica dos equipamentos.
- 4.10.6. A configuração compreenderá a realização dos ajustes de hardware e software necessários ao funcionamento dos dispositivos a fim de apresentarem a melhor performance de funcionamento possível.

4.10.7. Deverão ser feitas todas as atualizações de firmware ou qualquer outro software componente da solução, para a versão mais atualizada disponível ou a última compatível com as demais soluções de cada grupo e considerada estável.

4.10.8. Deverão ser habilitadas todas as licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados no projeto.

4.10.9. Deverá ser providenciado todo o acabamento necessário, evitando que restem fios e cabos expostos, preservando a qualidade estética do ambiente.

4.11. **Requisitos de Garantia**

4.11.1. A contratada deverá prestar serviços de garantia e assistência técnica, os quais deverão ser providos pelos fabricantes dos produtos ofertados, pelo período de vigência do contrato;

4.11.2. Manutenção corretiva de "hardware" dos produtos fornecidos, incluindo a reparação de eventuais falhas, mediante a substituição de peças e componentes por outros de mesma especificação, novos de primeiro uso e originais, de acordo com os manuais e normas técnicas específicas para os mesmos;

4.11.3. Atualizações corretivas e evolutivas de "software" e "firmware", incluindo pequenas atualizações de "release", reparos de pequenos defeitos ("bug fixing" e "patches");

4.11.4. Ajustes e configurações conforme manuais e normas técnicas do fabricante;

4.11.5. Demais procedimentos destinados a recolocar os equipamentos em perfeito estado de funcionamento;

4.11.6. Assistência técnica especializada para investigar, diagnosticar e resolver incidentes e problemas relativos aos produtos fornecidos;

4.11.7. Os serviços de garantia no prazo estabelecido no [\[ITEM 4.5\]](#) , para todos os componentes de "hardware" e de "software" ofertados na respectiva proposta, deverão ser comprovados pelo fabricante do equipamento por meio de "site", portal ou documentação para os componentes do Grupo I;

4.11.8. Os serviços de garantia no prazo de 60 (sessenta) meses, para todos os componentes de "hardware" e de "software" ofertados na respectiva proposta, deverão ser comprovados pelo fabricante do equipamento por meio de "site", portal ou documentação;

4.11.9. Os serviços de garantia e de assistência técnica deverão ser prestados pelo fabricante da solução no regime de 24 (vinte e quatro) horas dia durante os 7 (sete) dias da semana (24 x 7), sem qualquer ônus adicional ao contratante;

4.11.10. A troca de peças deverá ser realizada no **próximo dia** da chegada das peças no endereço do Hospital Universitário Lauro Wanderley (HULW-UFPA), conforme item [\[ITEM 4.14.2\]](#) ;

4.11.11. A contratada deverá disponibilizar canal de atendimento para abertura de chamados técnicos, por meio de número de telefone fixo ou número local (nas cidades onde se encontrarem instalados os equipamentos), ou ainda, poderá ser disponibilizado serviço de abertura de chamado via "site" ou "e-mail";

4.11.12. Para cada chamado técnico, a contratada deverá informar um número de controle (protocolo) para registro, bem como manter histórico de ações e atividades realizadas;

4.11.13. Os chamados técnicos serão classificados por criticidade, de acordo com o impacto no ambiente computacional do contratante, conforme prioridades enumeradas a seguir:

4.11.13.1. Prioridade Alta: Sistema indisponível ou com severa degradação de desempenho;

4.11.13.2. Prioridade Média: Sistema disponível, com mau funcionamento, que importe baixa degradação de desempenho ou comprometimento em um de seus elementos que importe em risco para a disponibilidade do sistema;

4.11.13.3. Prioridade Baixa: Sistema disponível, sem impacto em seu desempenho ou disponibilidade; consultas gerais sobre instalação, administração, configuração, otimização, "troubleshooting" ou utilização.

4.11.14. O nível de severidade será informado pelo CONTRATANTE no momento da abertura do chamado.

4.11.15. O CONTRATANTE poderá escalar os chamados para níveis mais altos ou baixos, de acordo com a criticidade do problema. Nesse caso, os prazos de atendimento e de solução, bem como os prazos e percentuais de multa, serão automaticamente ajustados para o novo nível de prioridade.

4.11.16. Os serviços de assistência técnica em garantia deverão atender, respectivamente, os seguintes prazos de atendimento inicial e de solução do incidente:

4.11.16.1. Os chamados de "Prioridade Alta" deverão ser atendidos em até 2 (duas) horas, com resolução do chamado ou solução de contorno em até 6 (seis) horas;

4.11.16.2. Os chamados de "Prioridade Média" deverão ser atendidos em até 8 (oito) horas com resolução do chamado ou solução de contorno em até 24 (vinte e quatro) horas;

4.11.16.3. Os chamados de "Prioridade Baixa" deverão ser atendidos em até 24 (vinte e quatro) com resolução do chamado ou solução de contorno em até 96 (noventa e seis) horas;

4.11.17. O prazo de atendimento começará a ser contado a partir da hora do acionamento do suporte via central de atendimento da contratada;

4.11.18. Entende-se por início de atendimento a hora de chegada do técnico de suporte ao local onde está o produto ou sua intervenção remota;

4.11.19. Entende-se por término do atendimento ou chamado atendido a ocorrência de um dos eventos abaixo relacionados:

4.11.19.1. Solução definitiva;

4.11.19.2. Solução de contorno e escalonamento do chamado para um nível de menor severidade, mediante prévia aprovação do contratante;

4.11.20. O encerramento do chamado será dado por servidor da equipe técnica do CONTRATANTE na conclusão dos serviços, após a disponibilização da solução para uso em perfeitas condições de funcionamento no local onde está instalada;

4.11.21. Caberá aos técnicos do fabricante ou da empresa autorizada pelo fabricante identificar os componentes, peças e materiais responsáveis pelo mau funcionamento dos produtos fornecidos;

4.11.22. Em caso de falhas irreversíveis de "hardware" ou impossibilidade de solução pela assistência técnica, a contratada deverá providenciar a troca por equipamento idêntico ou superior;

4.11.23. Casos em que se tornará obrigatória a substituição de equipamentos pela contratada;

4.11.24. Falha de componente de "hardware" que interrompa o perfeito funcionamento do equipamento;

4.11.25. Por questão de segurança, os equipamentos e "software" nunca deverão ser removidos das dependências do contratante sem a remoção de dados ou regras sigilosas;

4.11.26. No caso de troca do produto por defeito, não haverá qualquer ônus adicional para o contratante;

4.11.27. Relativamente à manutenção corretiva de "hardware" e "software";

4.11.28. Os componentes danificados deverão ser substituídos, entregues, instalados e configurados, de modo a deixar o equipamento em perfeitas condições de uso e com todas as funcionalidades operacionais, nas dependências do contratante, nos prazos de solução estabelecidos acima, sem a cobrança de quaisquer custos adicionais (frete, seguro, etc.);

4.11.29. Concluída a manutenção, a contratada fornecerá ao contratante, documento em que conste a identificação do chamado técnico, data e hora de início e término da assistência técnica, descrição dos serviços executados, indicação da peça e/ou componente eventualmente substituído, assim como relato referente às condições inadequadas ao funcionamento do equipamento ou sua má utilização, fazendo constar a causa e as medidas para a sua correção;

4.11.30. Durante todo o período de garantia, a contratada atualizará ou disponibilizará para "download", sem ônus adicionais para o contratante, os componentes de "softwares" necessários ao perfeito funcionamento dos produtos fornecidos, fornecendo as novas versões ou "releases" lançados. Os componentes de "softwares" tratados neste item incluem assinaturas, "software" de gerenciamento, "firmwares" de BIOS e "drivers";

4.11.31. Qualquer manutenção e/ou intervenção por solicitação da CONTRATADA ou do FABRICANTE, mesmo não implicando em inoperância do sistema ou alteração de suas características, deverá ser agendada e acordada previamente com o CONTRATANTE;

4.11.32. Os serviços deverão ser prestados por equipe técnica qualificada pelo fabricante do sistema;

4.11.33. A CONTRATADA não poderá impor qualquer limitação de quantitativo de chamados, seja diário, mensal, anual, ou de tempo de duração dos chamados, durante o período de prestação dos serviços.

4.11.34. O CONTRATANTE poderá acompanhar os chamados técnicos abertos pela contratada junto ao fabricante;

4.11.35. Será admitida a subcontratação dos serviços de garantia e assistência técnica, desde que previamente autorizada por escrito pelo CONTRATANTE, por empresa comprovadamente autorizada pelo fabricante dos equipamentos;

4.12. **Requisitos de Experiência Profissional**

4.12.1. A Contratada deverá ter experiência no mercado, executando serviços compatíveis com o objeto contratado, cuja comprovação poderá ser realizada com a apresentação de cópia de contratos firmados com Instituições Públicas ou Privadas;

4.12.2. A contratada deverá disponibilizar profissionais experientes, devidamente qualificados e certificados para a manutenção e disponibilização da solução, durante toda a vigência contratual;

4.12.3. As comprovações solicitadas nos itens [\[ITEM 4.12.1\]](#) e [\[ITEM 4.12.2\]](#) deverão ser apresentadas ainda na fase de habilitação;

4.13. **Requisitos de Formação da Equipe**

4.13.1. Requisito não aplicável a contratação.

4.14. **Requisitos de Metodologia de Trabalho**

4.14.1. As atividades serão desenvolvidas fisicamente no endereço abaixo:

4.14.2. Hospital Universitário Lauro Wanderley (HULW-UFPB). Endereço: Rua Tabelião Stanislaw Eloy, s/n, Castelo Branco, João Pessoa/PB – CEP 58.050-585.

4.14.3. As implantações de hardware e instalação de software deverão ocorrer segundo as boas práticas descritas pelo fabricante em manuais e executadas por profissionais com conhecimento sobre a solução adquirida.

4.15. **Requisitos de Segurança da Informação**

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

4.15.2. A CONTRATADA se compromete a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do contrato, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do contrato.

4.15.3. A CONTRATADA e seus técnicos comprometem-se a respeitar a Política de Segurança da Informação da EBSERH.

4.15.4. A CONTRATADA e seus técnicos comprometem-se a manter em caráter confidencial, mesmo após eventual rescisão do contrato, as informações obtidas e/ou registradas, dentre as quais:

4.15.4.1. as configurações de hardware e software decorrentes do processo de manutenção;

4.15.4.2. o processo de configuração dos equipamentos; e

4.15.4.3. quaisquer dados de que a CONTRATADA venha a ter conhecimento em decorrência da presente contratação, pertinentes a hardware, serviços, sistemas e aplicativos tanto da SETISD, como a EBSERH, cujo conhecimento por terceiros exponha o ambiente a riscos de invasão ou resulte na vulnerabilidade do mesmo.

4.15.5. Será firmado o Anexo A - Termo de Compromisso e Manutenção do Sigilo ([33642344](#)), contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e o Anexo B - Termo de Ciência ([33642348](#)), a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação.

4.16. **Outros Requisitos Aplicáveis**

4.16.1. Da Ata de Registro de preço

4.16.1.1. A adoção de Ata de Registro de Preço para esta contratação preterida, baseia-se no art. 3, inciso IV, do Decreto nº 7.892, de 23 de janeiro de 2013, que versa o seguinte:

Art. 3º O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:

I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;
II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;

III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; ou

IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

4.16.1.2. Outrossim, cada fase possui a disponibilização de novos serviços à comunidade amapaense, todavia, não é possível deduzir o nível de consumo desses novos serviços e, por seu conseguinte, seu impacto frente ao ambiente computacional do HULW-UFPB.

4.16.1.3. Destarte, devido a incertezas quanto ao poder computacional necessário para o atendimento de demandas institucionais mediante ao aumento dos consumos de serviços assistenciais, reiteremos o alinhamento com o art.3, inciso IV, do decreto 7.892.

4.16.1.4. Será permitidas adesões de registro de preço na origem (Intenção de Registro de Preço) e adesões posteriores ao processo de licitação (carona) apenas para órgão assistidos pela Lei 13.303 (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);

4.16.1.5. Necessidade de formalização de termo de contrato ou instrumento equivalente;

4.16.1.6. Diante da necessidade de garantia sobre os bens adquiridos e serviços, torna-se indispensável a formalização de contrato entre o HULW-UFPB e a(s) empresa(s) vencedoras da licitação.

4.16.2. Da Subcontratação

4.16.2.1. Com o intuito da execução do serviço ser realizada de forma mais rápida e usando menos recurso financeiro possível, **não será permitida a subcontratação.**

4.16.3. Da Alteração Subjetiva

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

4.16.4. Da garantia de execução

4.16.4.1. Não será exigida garantia sobre a execução da contratação aqui pleiteada.

5. RESPONSABILIDADES

5.1. Deveres e responsabilidades da CONTRATANTE

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

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

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

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

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

- 5.1.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TI;
- 5.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável; e
- 5.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração;
- 5.1.9. Receber o objeto no prazo e condições estabelecidas neste Termo;
- 5.1.10. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes deste Termo e da proposta, para fins de aceitação e recebimento definitivo;
- 5.1.11. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;
- 5.1.12. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;
- 5.1.13. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos neste Termo;

5.2. **Deveres e responsabilidades da CONTRATADA**

- 5.2.1. Indicar formalmente e por escrito, no prazo máximo de 05 (cinco) dias úteis após a assinatura do contrato, junto à contratante, um preposto idôneo com poderes de decisão para representar a contratada, principalmente no tocante à eficiência e agilidade da execução do objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato;
- 5.2.2. Na hipótese de afastamento do Preposto definitivamente ou temporariamente, a CONTRATADA deverá comunicar ao Gestor do Contrato por escrito o nome e a forma de comunicação de seu substituto até o próximo dia útil.
- 5.2.3. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- 5.2.4. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;
- 5.2.5. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;
- 5.2.6. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- 5.2.7. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TI;
- 5.2.8. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e
- 5.2.9. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados à Administração;
- 5.2.10. Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).
- 5.2.11. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da contratante;
- 5.2.12. Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão;
- 5.2.13. A Contratada deve cumprir todas as obrigações constantes neste Termo, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

- 5.2.14. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste Termo e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;
- 5.2.15. O objeto deve estar acompanhado do manual do usuário, com uma versão em português e da relação da rede de assistência técnica autorizada.
- 5.2.16. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);
- 5.2.17. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;
- 5.2.18. Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega dos itens, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;
- 5.2.19. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- 5.2.20. A CONTRATADA deverá, quando da assinatura da Ata do Pregão, assinar um termo de responsabilidade pela garantia dos equipamentos, independente da garantia do fabricante.
- 5.2.21. Garantir e disponibilizar, pelo tempo de garantia, as atualizações necessárias aos bens contratados, se for o caso.
- 5.2.22. Prestar informações e os esclarecimentos que venham a ser solicitados pela Contratante por intermédio de Preposto designado para acompanhamento do contrato nos seguintes prazos, a contar da solicitação:
- 5.2.23. em até 2 dias úteis nas capitais; e
- 5.2.24. em até 4 dias úteis nas demais localidades.
- 5.2.25. Assumir inteira responsabilidade técnica e operacional do objeto contratado, não podendo, sob qualquer hipótese, transferir a outras empresas a responsabilidade por quaisquer problemas relacionados ao fiel cumprimento do contrato;
- 5.2.26. Caso o problema de funcionamento do bem e ou serviço detectado tenha a sua origem fora do escopo do objeto contratado, a Contratada repassará para a Contratante as informações técnicas com a devida análise fundamentada que comprovem o fato, sem qualquer ônus para a Contratante.
- 5.3. **Deveres e responsabilidades do órgão gerenciador da ata de registro de preços**
- 5.3.1. Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Pregão;
- 5.3.2. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;
- 5.3.3. Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:
- 5.3.4. As formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e
- 5.3.5. Definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;
- 5.3.6. Definir mecanismos de controle de fornecimento da solução de TI, observando, dentre outros:
- 5.3.7. A definição da produtividade ou da capacidade mínima de fornecimento da solução de TI;
- 5.3.8. 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
- 5.3.9. As regras para a substituição da solução registrada na Ata de Pregão, garantida a realização de Prova de Conceito, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica;
- 5.3.10. É da competência do órgão gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado na ata de pregão (art. 5º, inciso X, do Decreto nº 7.892/2013), exceto nas hipóteses em que o descumprimento disser

respeito às contratações dos órgãos participantes, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 6º, Parágrafo único, do Decreto nº 7.892/2013)

5.3.11. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

6. MODELO DE EXECUÇÃO DO CONTRATO

<O Modelo de Execução do Contrato deverá contemplar as condições necessárias ao fornecimento da solução de TIC, observando os itens a seguir>.

6.1. Rotinas de Execução

6.1.1. Realização da Reunião Inicial

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

6.1.1.2. O representante legal da contratada deverá entregar o Termo de Referência - SEI SETISD/SUP/HULW-UFPB ([33062763](#)) e o Anexo B - Termo de Ciência ([33642348](#)), contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade;

6.1.1.3. O representante legal da contratada deverá apresentar o um Plano de Implantação, Projeto Executivo ou documento equivalente, doravante denominado Plano de Trabalho;

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

6.1.1.5. O suporte técnico deverá ser de acordo com o [ITEM 4.4](#) ;

6.1.2. Procedimentos para encaminhamento e controle de solicitações

6.1.2.1. As questões administrativas formais ocorridas durante a execução do contrato serão tratadas através de ofício.

6.1.2.2. Questões administrativas ou operacionais cotidianas durante a execução do contrato poderão ser tratadas através de mensagem eletrônica (e-mail), telefone, aplicativo de mensagens ou outro meio informatizado que armazene o histórico da tramitação das solicitações e respostas.

6.1.2.3. O HULW-UFPB comunicar-se-á com a CONTRATADA por intermédio do seu preposto a ser indicado em até 5 (cinco) dias após a assinatura do contrato;

6.1.2.4. A comunicação entre a Gestão e/ou Fiscalização Contratual e a CONTRATADA será por meio escrito sempre que se entender necessário o registro de ocorrência relacionado com a execução da contratação;

6.1.2.5. Para comunicação eletrônica disponibiliza-se o endereço: setisd.hulw-ufpb@ebserh.gov.br e uisti.hulw-ufpb@ebserh.gov.br

6.1.3. Forma de execução e acompanhamento dos serviços

6.1.3.1. A empresa contratada deve seguir as boas práticas de gestão de projeto, bem como as recomendações presentes nos manuais do fabricante da solução a ser implantada/atualizada;

6.1.4. Prazos, horários de fornecimento de bens ou prestação dos serviços

6.1.4.1. Serão definidos prazos, horários de fornecimento de bens ou prestação dos serviços sendo que a entrega de todos os produtos deverá ocorrer em até no máximo 30 (trinta) dias corridos a partir da data de assinatura do contrato.

6.1.4.2. A implantação completa da solução deverá ser concluída em até 30 (trinta) dias corridos após a entrega dos equipamentos.

6.1.5. Locais de entrega

6.1.5.1. O(s) equipamento(s) deverá(ão) ser entregue(s) e instalado(s) nas dependências da HULW-UFPB, mediante agendamento com antecedência mínima de 24 horas, sob o risco de não ser autorizada, na Rua Estanislau Eloy, s/nº - Bairro Castelo Branco

João Pessoa-PB, CEP 58050-585, térreo, local onde está situado o Setor de Tecnologia da Informação e Saúde Digital do HULW-UFPB. A entrega e instalação deverá ser realizada em dias úteis em horário previamente acordado entre as partes.

6.1.6. Documentação mínima exigida

6.1.6.1. A Contratada deverá fornecer a documentação mínima exigida conforme segue:

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

6.1.6.3. Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas.

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

6.2.1. Os bens e serviços serão recebidos:

6.2.1.1. Provisoriamente, após a entrega dos bens ou execução dos serviços, mediante **Termo de Recebimento Provisório**, declaração formal de que os serviços foram prestados ou os bens foram entregues, para posterior análise das conformidades e qualidade baseada nos requisitos e nos critérios de aceitação dispostos neste Termo de Referência, Edital, seus anexos e da proposta;

6.2.1.2. Definitivamente, após implementação e implantação total da solução, composta pelo conjunto de todos bens e serviços constantes em cada GRUPO, observando-se disposto no **item 4.5.3** (Requisitos Temporais) deste Termo de Referência e após análise e verificação das conformidades e qualidades baseadas nos requisitos e nos critérios de aceitação dispostos neste Termo de Referência, Edital, seus anexos e da proposta, mediante **Termo de Recebimento Definitivo**, declaração formal de que os serviços prestados ou bens fornecidos atendem aos requisitos estabelecidos e aos critérios de aceitação;

6.2.1.3. O prazo disposto no subitem anterior terá início a partir da comunicação, por parte da CONTRATADA, de conclusão de implementação e implantação da solução, deixando-a plenamente operacional e de acordo com os requisitos e critérios de aceitação dispostos neste Termo de Referência, Edital, seus anexos e da proposta;

6.2.2. O conjunto de *procedimentos de instalação e configuração*, a ser previsto no Plano de Trabalho, deverá compreender, no mínimo, mas não exclusivamente, as seguintes etapas:

6.2.2.1. Instalação dos softwares em sua última versão estável;

6.2.2.2. Atualização de firmwares e drivers para sua última versão estável;

6.2.2.3. Instalação dos appliance do firewall;

6.2.2.4. Instalação e aplicação de todas as licenças ofertadas, caso necessário;

6.2.2.5. Migração de regras do Firewall em produção para os novos firewalls (PA-3220);

6.2.2.6. Configuração de toda a infraestrutura de rede necessária, virtual, física e lógica;

6.2.2.7. Configuração dos recursos de alta disponibilidade;

6.2.2.8. Configuração de identificação de usuário;

6.2.2.9. Configuração de armazenamento;

6.2.2.10. Configuração das políticas de segurança e políticas de backup da informação;

6.2.2.11. Testes de validação da instalação e configuração;

6.2.3. Após a conclusão da implantação da solução, a CONTRATADA deverá entregar um relatório as-built, devendo conter, no mínimo, mas não exclusivamente:

6.2.3.1. Todos os itens do Plano de Trabalho;

6.2.3.2. Características dos serviços;

6.2.3.3. Topologias e arquitetura final da solução implantada e operacional;

6.2.3.4. Atividades operacionais;

6.2.3.5. Dados para abertura de chamados e escalation list;

6.2.3.6. Procedimentos para interrupções programadas;

6.2.3.7. Indicação de forma detalhada das condições de rollback de cada mudança realizada no ambiente do HULW-UFPB.

6.3. Mecanismos formais de comunicação

6.3.1. Encontram-se descritas no item [\[ITEM 4.4.4.3\]](#)

6.4. Manutenção de Sigilo e Normas de Segurança

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

6.4.2. O Anexo A - Termo de Compromisso e Manutenção do Sigilo ([33642344](#)), contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e Anexo B - Termo de Ciência ([33642348](#)), a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação.

7. **MODELO DE GESTÃO DO CONTRATO**

7.1. Critérios de Aceitação

7.1.1. Por se tratar de aquisição de equipamentos, os procedimentos de teste e inspeção se basearão em testes de performance, além do acompanhamento durante a utilização dos equipamentos. Ao receber os equipamentos deverá ser realizada a inspeção para verificar se todos os itens estão sendo entregues pela contratada, considerando os aspectos quantitativos e qualitativos, assim como período de validade das licenças. Durante a configuração/instalação dos equipamentos, poderão ser feitos testes de performance, utilizando-se de softwares específicos. Os equipamentos deverão ser utilizados conforme instruções do fabricante e as orientações da contratada, reduzindo assim os riscos de danos materiais.

7.1.2. Não serão aceitos bens e/ou serviços ofertados para este certame em desacordo com o [\[ITEM 4.8\]](#) , salvo a critério da administração, após análise da equipe técnica da instituição;

7.1.3. Não será aceito o fornecimento parcial de bens e serviços deste certame, relacionados ao GRUPO 01;

7.1.4. Será avaliada, finalmente, a funcionalidade integral da solução contratada no GRUPO 01;

7.1.5. Somente serão aceitos equipamentos e softwares novos, sem uso e em linha de fabricação. Não serão aceitos equipamentos remanufaturados, NFR (Not For Resale) ou de demonstração.

7.1.6. Os equipamentos deverão ser entregues nas caixas lacradas pela CONTRATADA, não sendo aceitos equipamentos com caixas violadas;

7.1.7. A CONTRATADA deverá fornecer todas as chaves de licenças de todos os softwares segundo as requisitos e especificações técnicos [\[ITEM 4.8\]](#) ;

7.1.8. A CONTRATADA deverá fornecer comprovação dos contratos de garantia estendida do fabricante e de suporte pelo período contratado de 60 (sessenta) meses para os componentes do Grupo I;

7.1.9. Não serão aceitos equipamentos ou software que não estejam na linha de produção na data do certame com previsão de fim de vida ou nos modos “ end of sale ”, “ end of life ” e “ end of support ”;

7.1.10. Deverá ser fornecido link de acesso para comprovação das informações no site do fabricante do software e/ou equipamentos;

7.1.11. As chaves fornecidas pela CONTRATADA deverão estar disponíveis para consulta, a qualquer tempo;

7.1.12. O recebimento definitivo somente será dado após sanadas todas as ressalvas feitas - quando houver - no Termo de Recebimento Provisório.

7.1.13. Além disso, comprovação da entrega e o efetivo cumprimento de todas as exigências presente nas especificações técnicas (item 4.8), assim como depois de implantada as soluções/itens;

7.1.14. Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital;

7.1.15. Os equipamentos, softwares e serviços serão recebidos:

7.1.16. Provisoriamente, no prazo de 10 (dez) dias úteis, por servidor designado da Unidade de Infraestrutura, Suporte e Segurança da Tecnologia da Informação, para efeito de verificação da conformidade com as especificações e condições da contratação;

7.1.17. Definitivamente, após a verificação da conformidade do objeto entregue com as especificações e condições da contratação e consequente aceitação, no prazo de 20 (vinte) dias úteis, contados da data do recebimento provisório, com a certificação da nota fiscal por servidor designado da Unidade de Infraestrutura, Suporte e Segurança da Tecnologia da Informação, pelo gestor do contrato ou pela comissão de recebimento designada.

7.1.18. A CONTRATANTE se reserva o direito de recusar, formal e justificadamente, qualquer material, bem ou serviço que não esteja em conformidade com o ajustado;

7.1.19. A CONTRATANTE poderá rejeitar, total ou em partes, a solução que não atender aos Requisitos de Arquitetura Tecnológica descritas no [ITEM 4.8](#) e as Rotinas de Execução descritas [ITEM 6](#) ;

7.1.20. A CONTRATADA deve apresentar documentação que comprove parceria com o fabricante da solução.

7.2. Procedimentos de Teste e Inspeção

7.2.1. Verificação quanto ao atendimento dos requisitos e especificações técnicas para cada item individualmente, o funcionamento a contento da solução como um todo, de forma que os itens individualmente devem estar eficiente e eficazmente instalados, configurados e operacionais, e, no conjunto da solução integrada, efetividade no atendimento dos objetivos da administração para a solução contratada;

7.2.2. Acesso ao site da fabricante para averiguação, por meio das chaves de licenças, service tags , part numbers , números de série ou equivalentes, da validade do serviço de garantia e suporte;

7.2.3. Verificação por meio de link enviado pela CONTRATADA, no site do(s) fabricante(s), se os produtos fornecidos não estão na situação de “ end of sale ”, “ end of life ” ou “ end of support ”;

7.2.4. Será realizado abertura de chamado teste por intermédio dos canais de atendimento;

7.2.5. Verificação por meio de link enviado pela CONTRATADA, no site do(s) fabricante(s), compatibilidade do software com os hardwares ofertados.

7.3. Níveis Mínimos de Serviço Exigidos

7.3.1. Deve atender aos requisitos e especificações do item (especificações técnicas);

7.3.2. Serão exigidos os Níveis Mínimos de Serviço seguintes:

7.3.2.1. Todo o ônus financeiro referente a prestação do suporte será custeado pela CONTRATADA;

7.3.2.2. O atendimento aos chamados deverá obedecer à seguinte classificação quanto ao nível de severidade:

Severidade	Descrição	Tipo de atendimento	Tempo de atendimento	Tempo de solução ou de contorno
Crítica	Chamados referentes a emergências ou problema crítico, caracterizados pela existência de ambiente paralisado.	Remoto	No máximo 2 (duas) horas após a abertura do chamado.	No máximo, até o próximo dia útil após o início do atendimento do chamado
Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho.	Remoto	No máximo 3 (três) horas após a abertura do chamado.	No máximo, até o segundo dia útil após o início do atendimento do chamado
Média	Chamados referentes a situações de baixo	Remoto	No máximo 4 (quatro) horas após a	No máximo, até o terceiro dia útil após

Severidade	Descrição	Tipo de atendimento	Tempo de atendimento	Tempo de solução ou de contorno
	impacto ou para aqueles problemas que se apresentem de forma intermitente, incluindo os casos em que haja necessidade de substituição de componentes) que possuam redundância		abertura do chamado	o início do atendimento do chamado.
Baixa	Chamados com o objetivo de sanar dúvidas quanto ao uso ou à implementação do produto	Remoto	No máximo 24 (vinte e quatro) horas após a abertura do chamado.	No máximo em cinco dias úteis após a abertura do chamado.

7.3.3. Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento. Os chamados serão atendidos inicialmente de forma remota com atendimento iniciado de acordo com o prazo estipulado na tabela acima máximo com vistas a aplicar solução ou medida de contorno até o prazo definido na coluna “Tempo de solução ou de contorno” da referida tabela.

7.3.4. Os atendimentos de Severidade 1 e 2 não poderão ser interrompidos até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis;

7.3.5. Os chamados classificados com Severidade 4 serão atendidos das 08h00 às 18h00, de segunda-feira a sexta-feira, horário de Brasília, exceto feriados;

7.3.6. O suporte técnico deverá ser prestado em português ou deverá ser oferecido um tradutor.

7.3.7. Manutenções (para todos os itens):

7.3.7.1. A CONTRATADA deverá prover, sempre que necessário, todas as correções e/ou atualizações dos softwares e hardwares instalados, tais como: nível de firmware e microcódigos, que permitam melhorar as funcionalidades dos equipamentos, bem como mantê-los compatíveis com os demais componentes de hardware e software dos Centros de Dados do CONTRATANTE, sem ônus adicional para a CONTRATANTE;

7.3.7.2. A CONTRATADA deverá dar conhecimento à CONTRATANTE, através de e-mail, da existência de alterações nas configurações dos equipamentos. A CONTRATANTE avaliará o impacto dessas alterações e agendará a realização da manutenção do equipamento ou software, tanto do hardware quanto do firmware instalados, sendo de responsabilidade da CONTRATADA prover todas as correções e/ou atualizações necessárias;

7.3.7.3. No caso de manutenções em que haja risco de indisponibilidade total ou parcial dos equipamentos, a CONTRATANTE deverá ser previamente notificada para que se proceda à aprovação e o agendamento da manutenção em horário conveniente a CONTRATANTE;

7.3.7.4. Caso a CONTRATANTE identifique a necessidade de manutenção em algum equipamento, a CONTRATADA será informada, o agendamento deverá ser acordado com a CONTRATANTE;

7.3.7.5. Correrá por conta exclusiva da CONTRATADA, a responsabilidade pelo deslocamento do seu técnico ao local da instalação do equipamento, bem como pela retirada e entrega do equipamento e peças de reposição, além de todas as despesas de transporte, frete e seguro correspondente;

7.3.7.6. Para os equipamentos ofertados, a CONTRATADA deverá prestar, durante o período de garantia, suporte técnico, tanto do hardware quanto do firmware e softwares instalados, observando os níveis de serviço especificados neste Contrato;

7.3.7.7. Em qualquer hipótese (e ainda que não seja o fabricante dos equipamentos) a CONTRATADA deverá possuir acesso para suporte técnico de 2º e 3º níveis, bem como aos firmwares e microcódigos dos equipamentos, de forma a prestar os serviços de manutenção e assistência técnica, sem ônus adicional para a CONTRATANTE;

7.3.8. A CONTRATANTE deverá disponibilizar recursos humanos necessários às atividades de gestão e fiscalização do contrato, inclusive quanto à qualificação técnica e disponibilidade de tempo para aplicação das listas de verificação e roteiros de testes:

Função	Quantidade	Atribuições
Gestor do Contrato	1	Colaborador com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente.
Fiscal Requisitante	1	Colaborador representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista técnico-funcional da Solução de Tecnologia da Informação.
Fiscal Técnico	1	Colaborador representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato.
Fiscal Administrativo	1	Colaborador representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos.

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

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

7.4.1.1. falhar na execução do contrato, pela inexecução, total ou parcial, de quaisquer das obrigações assumidas na contratação;

7.4.1.2. ensejar o retardamento da execução do objeto;

7.4.1.3. fraudar na execução do contrato;

7.4.1.4. comportar-se de modo inidôneo; ou

7.4.1.5. cometer fraude fiscal.

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

7.4.2.1. Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

7.4.2.2. Multa nos seguintes casos:

7.4.2.2.1. 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

7.4.2.2.2. 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;

7.4.2.2.3. 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

7.4.2.2.4. 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

7.4.3. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si, e se somarão nos seguintes casos:

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

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

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

7.4.3.4. A Sanção de impedimento de licitar e contratar prevista no subitem anterior também é aplicável em quaisquer das hipóteses previstas como infração administrativa neste Termo de Referência.

7.4.3.5. As sanções previstas nos subitens acima poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

7.4.4. O não atendimento dentro do prazo estabelecido para o chamado ou interrupção do atendimento de um chamado por parte da CONTRATADA, que não tenha sido previamente autorizada pelo CONTRATANTE ensejará aplicação de multa à CONTRATADA, conforme o nível de severidade do mesmo:

7.4.4.1. Severidade 1 – 0,5% (cinco décimos por cento) do valor constante no contrato para o item (equipamento) correspondente, por dia de atraso;

7.4.4.2. Severidade 2 – 0,4% (quatro décimos por cento) do valor constante no contrato para o item (equipamento) correspondente, por dia de atraso;

7.4.4.3. Severidade 3 – 0,2% (dois décimos por cento) do valor constante no contrato para o item (equipamento) correspondente, por dia de atraso;

7.4.4.4. Severidade 4 (onde se aplicar) – 0,1% (um décimo por cento) do valor constante no contrato para o item (equipamento) correspondente, por dia de atraso.

7.4.5. Sanções e Glosas:

ID	Ocorrência	Glosa/Sanção
1	Não comparecer injustificadamente à Reunião Inicial.	Advertência
2	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A Contratada ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais, e multa de 0,5% do valor da contratação.
3	Ter praticado atos ilícitos visando frustrar os objetivos da licitação	A Contratada será declarada inidônea para licitar e contratar com a Administração.
4	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
5	Não executar total ou parcialmente os serviços previstos no objeto da contratação.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual e Multa de 0,5% sobre o valor total do Contrato.
6	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por até de 30 dias, sem comunicação formal ao gestor do Contrato.	Multa de 0,5% sobre o valor total do Contrato. Em caso de reincidência, configura-se inexecução total do Contrato por parte da empresa, ensejando a rescisão contratual unilateral.

ID	Ocorrência	Glosa/Sanção
7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por mais de 30 (trinta) dias, sem comunicação formal ao gestor do contrato.	A contratada será declarada inidônea para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
8	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 24 horas úteis.	Multa de 0,4% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 10 dias úteis
9	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas, etc).	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na RLCE 2.0.
10	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado na fase de levantamento de requisitos e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na RLCE 2.0.
11	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na RLCE 2.0
12	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na RLCE 2.0

7.4.6. Também ficam sujeitas às penalidades da RLCE 2.0 (Capítulo III), as empresas ou profissionais que:

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

7.4.6.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

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

7.4.7. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na RLCE 2.0.

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

7.4.9. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

7.4.10. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

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

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

7.4.13. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

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

7.4.15. As penalidades serão obrigatoriamente registradas no SICAF.

7.5. Do Pagamento

7.5.1. O pagamento será efetuado pela CONTRATANTE no prazo de 30 dias, contados do recebimento da Nota Fiscal/Fatura, por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

7.5.2. O processo para pagamento deve observar o disposto na seção Requisitos Temporais e deverá ser executado, conforme o disposto na seção 9 (ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO) em seus subitens;

7.5.3. Consta no item 4.5.3 (seção dos Requisitos Temporais) o detalhamento das etapas ou fases da solução a ser contratada, com os serviços e bens que compõem a solução;

7.5.4. Quando houver glosa parcial dos serviços, a contratante deverá comunicar a empresa para que emita a nota fiscal ou fatura com o valor exato dimensionado.

7.5.5. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que a CONTRATANTE atestar a execução do objeto do contrato.

7.5.6. A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do serviço, conforme previsto neste Termo de Referência.

7.5.7. Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais.

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

7.5.9. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

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

7.5.10.1. o prazo de validade;

7.5.10.2. a data da emissão;

7.5.10.3. os dados do contrato e da CONTRATANTE;

7.5.10.4. o período de prestação dos serviços;

7.5.10.5. o valor a pagar; e

7.5.10.6. eventual destaque do valor de retenções tributárias cabíveis.

7.5.11. Nos termos do item 1, do Anexo VIII-A da Instrução Normativa SEGES/MP no 05, de 2017, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

7.5.11.1. não produziu os resultados acordados;

7.5.11.2. deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

7.5.11.3. deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

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

7.5.13. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

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

7.5.15. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa no 3, de 26 de abril de 2018.

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

7.5.17. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.

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

7.5.19. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da CONTRATANTE.

7.5.20. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1991, nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.

7.5.21. É vedado o pagamento, a qualquer título, por serviços prestados ou fornecimento de bens, à empresa privada que tenha em seu quadro societário servidor público da ativa da CONTRATANTE, com fundamento na Lei de Diretrizes Orçamentárias vigente.

7.5.22. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

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

VP = Valor da parcela a ser paga.

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

I = (TX)	I=(6/100) / 365	I = 0,00016438
		TX = Percentual da taxa anual = 6%

7.5.23. Para os serviços a contratada deverá peticionar à fiscalização a medição dos serviços prestados, via Sistema Eletrônico de Informações – SEI, apresentando, além do Relatório de despesas, a documentação obrigatória (certidões negativas municipal, estadual, união, trabalhista, regularidade FGTS e outros documentos a critério da fiscalização);

7.5.24. A contratada deve então emitir a Nota Fiscal ou a Fatura e solicitar, via ofício, o pagamento (no mesmo processo eletrônico de apresentação da documentação obrigatória) e encaminhar ao Gestor do Contrato;

7.5.25. Caso a contratada não tenha procedido o mencionado cadastro como usuário externo no referido sistema, não será possível a realização do ateste.

8. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1. Conforme o art 7 do Regulamento de Licitações e Contratos da EBSERH, temos o seguinte apontamento:

Art. 7º O valor estimado do procedimento licitatório será sigiloso, sem prejuízo da divulgação do detalhamento dos quantitativos e das demais informações necessárias para a elaboração das propostas, facultando-se sua publicidade, mediante justificativa.

§ 1º Para fins do disposto no caput, o valor estimado para a contratação será tornado público apenas após o encerramento da etapa de julgamento das propostas.

§ 2º Nas hipóteses em que forem adotados os critérios de julgamento por maior desconto ou por melhor técnica, a estimativa de preços deverá constar do instrumento convocatório.

8.2. Destarte, foi criado o processo SEI nº [23539.013127/2023-11](#) com a estimativa de valor.

9. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

A aquisição está prevista no Plano de Aplicação de Recursos 2023 e no Contrato de Objetivos 2023 e enquadrada nos limites orçamentários previstos para o exercício, deverá ser atendido com Recursos do Orçamento de 2023 e demais fontes que vierem a compor o orçamento deste nosocômio.

Do cronograma financeiro:

Etapa	Descrição	Prazo	Início da Contagem	Pagamento por item (%) do prazo	(%) Execução Financeira (Valor Global Estimado)
1	Assinatura do contrato	-	-	0%	0%
2	Reunião inicial	5 dias	dias úteis contados a partir da etapa 1.	0%	0%
3	Emissão de Ordem de fornecimento de Bens/ serviços	15 dias	dias úteis, contados a partir da etapa 1.	0%	0%
4	Entrega de bens	60 dias	dias corridos, contados a partir da etapa 1 (um), podendo ser prorrogado por até 30 (trinta) dias corridos, mediante justificativa da CONTRATADA e aprovação pela CONTRATANTE.	0%	0%
5	Instalação e testes	30 dias	dias corridos após a entrega dos equipamento.	0%	0%

Etapa	Descrição	Prazo	Início da Contagem	Pagamento por item (%) do prazo	(%) Execução Financeira (Valor Global Estimado)
6	Transferência de conhecimento	5 dias	dias úteis, contados a partir da conclusão da etapa 5.	0%	0%
7	Emissão do termo de Recebimento provisório	30 dias	dias corridos, contados a partir da etapa 6.	0%	0%
8	Termo de Recebimento Definitivo	15 dias	dias corridos após a conclusão da etapa 7 (a partir desta etapa se inicia a contagem do prazo de garantia).	0%	0%
9	Emissão de nota fiscal	5 dias	dias corridos após a conclusão da etapa 8.	0%	0%
10	Pagamento	30 dias	dias úteis, após o recebimento da Nota fiscal	100%	100%

10. DA VIGÊNCIA DO CONTRATO

10.1. O contrato vigorará por 12 (doze) meses, contados a partir da data da sua assinatura, podendo ser prorrogado por períodos iguais e sucessivos, limitado a 60 (sessenta) meses, desde que haja preços e condições mais vantajosas para a Administração, nos termos do art. 147 da RLCE 2.0.

10.2. A prorrogação do contrato dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada da realização de pesquisa de mercado que demonstre a vantajosidade dos preços contratados para a Administração.

11. DO REAJUSTE DE PREÇOS (QUANDO APLICÁVEL)

11.1. Por se tratar da aquisição de um bem de TI, será utilizado o Índice de Custos da Tecnologia da Informação (ICTI) - IPEA.

11.2. Os preços inicialmente contratados são fixos e irredutíveis no prazo de um ano contado da data limite para a apresentação das propostas;

11.3. Após o interregno de um ano, e independentemente de pedido da Contratada, os preços iniciais serão reajustados, mediante a aplicação, pela Contratante exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, com base na seguinte fórmula (art. 5º do Decreto n.º 1.054, de 1994):

$R = V (I - I^0) / I^0$, onde:	
R	Valor do reajuste procurado
V	Valor contratual a ser reajustado
I^0	Índice inicial-refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta na licitação
I	Índice relativo ao mês do reajustamento

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

11.5. 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.

11.6. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

11.7. 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.

11.8. 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.

11.9. O reajuste será realizado por apostilamento.

12. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. Regime, Tipo e Modalidade da Licitação

12.1.1. Da natureza dos bens e/ou serviços

12.1.1.1. Quanto ao tipo, em conformidade com a Lei nº14.133/2021, o OBJETO pretendido enquadra-se como “BEM COMUM” por apresentar, independentemente de sua complexidade, “padrões de desempenho e qualidade que possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado”.

12.1.2. Do regime de execução

12.1.2.1. De acordo com o art 4º da RLCE 2.0 , enquadra-se a pretensão contratual no tipo Compra a ser processada mediante Sistema de Registro de Preços. Já o regime de execução do objeto qualifica-se como indireto, na modalidade empreitada por preço global, pois os órgãos e entidades participantes dessa contratação sabem exatamente a qualidade do bem a ser adquirido, bem como a quantidade exata que irá atender a necessidade de sua instituição.

12.1.3. Do Tipo e Critério de Julgamento

12.1.3.1. Na forma do art. 23 da IN SGD/ME nº94/2022, são apresentados a seguir os critérios técnicos para avaliação e julgamento das propostas para a fase de SELEÇÃO DO FORNECEDOR, observando-se as disposições normativas e legais aplicáveis às contratações públicas.

12.1.4. Modalidade, tipo de licitação, modo de disputa

12.1.5. De acordo com a Lei nº 14.133/21, esta licitação deve ser realizada na modalidade de PREGÃO NA FORMA ELETRÔNICA, com julgamento pelo critério de MENOR PREÇO.

12.1.6. O Modo de Disputa será ABERTO conforme definindo no Lei nº 14.133/21.

12.1.7. Intervalo entre lances

12.1.7.1. 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, será de 0,75%.

12.1.8. Da utilização do Sistema de Registro de Preços

12.1.8.1. O Decreto nº 11.464/22, a utilização do Sistema de Registro de Preços deve enquadrar-se nas seguintes hipóteses:

Art. 3º O SRP poderá ser adotado quando a Administração julgar pertinente, em especial:

I - quando, pelas características do objeto, houver necessidade de contratações permanentes ou frequentes;

II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, como quantidade de horas de serviço, postos de trabalho ou em regime de tarefa;

III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas;

IV - quando for atender a execução descentralizada de programa ou projeto federal, por meio de compra nacional ou da adesão de que trata o § 2º do art. 32; ou

V - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

12.1.8.2. Por outro lado, de acordo com o Decreto 11.464/22, a existência de preços registrados não obriga a Administração Pública a contratar, facultando-se a realização de licitação específica para a aquisição pretendida, assegurada preferência ao fornecedor registrado em igualdade de condições.

12.1.8.3. Conforme o art. 3 do Decreto nº 11.464/22, de 23 de janeiro de 2013, justificamos a necessidade de criação de Ata de Registro de Preço embasado no inciso I conforme demanda apresentada;

12.1.8.4. O quantitativo necessário também atende ao exposto neste termo.

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

12.2.0.1. Por fim, destaca-se que não será aplicada a cota de reserva de 25% para empresas classificadas como microempresas (ME) e empresas de pequeno porte (EPP), prevista no inciso I do art. 48 da Lei Complementar nº 123/2006 e no Decreto nº 8.538/2015. Como motivação para a não aplicação dessa cota, utiliza-se a própria orientação constante nos modelos de Termo de Referência elaborados pela Advocacia Geral da União (AGU). Em tais modelos, enfatiza-se que há a possibilidade de não utilização de tal cota de reserva nas hipóteses do art. 10, incisos I, II e IV do Decreto nº 8.538, de 2015, transcritos a seguir:

I – se não houver o mínimo de três fornecedores competitivos enquadrados como microempresas [...] capazes de cumprir as exigências estabelecidas no instrumento convocatório;

II - o tratamento diferenciado e simplificado para as microempresas e as empresas de pequeno porte não for vantajoso para a administração pública ou representar prejuízo ao conjunto ou complexo do objeto a ser contratado, justificadamente;

(...)

IV - o tratamento diferenciado e simplificado não for capaz de alcançar, justificadamente, pelo menos um dos objetivos previstos no art. 1º.

12.2.0.2. Cumpre também enfatizar que se considera “não vantajosa a contratação” quando: I - resultar em preço superior ao valor estabelecido como referência; ou II - a natureza do bem, serviço ou obra for incompatível com a aplicação do benefício (Decreto nº 8.538, de 2015, art. 10, parágrafo único)."

12.2.0.3. Com fulcro no art. 10, inciso II do Decreto nº 8.538, de 2015, justifica-se a não utilização da cota de reserva de 25% para este processo centralizado de aquisição. Isso porque, a fixação de cotas para a presente contratação apresenta riscos ao alcance dos resultados pretendidos, em especial no que tange à obtenção de ganho de escala. A redução do potencial de ganho de escala na comercialização dos itens do certame, que se configuram como produtos altamente padronizados, podem trazer impactos negativos ao preço final do processo de licitação centralizada, o que vai de encontro a um dos principais objetivos das licitações conduzidas pela Central de Compras, que é reduzir o preço dos bens contratados em função do ganho de escala com o número expressivo de itens adquiridos de forma centralizada em nome de diversos Órgãos Participantes. Além disso, espera-se que a empresa vencedora do certame em questão tenha estrutura para realizar a distribuição de um volume expressivo de equipamentos ao longo de todo o território nacional. Isso, a nosso ver, também não é compatível com o porte das empresas beneficiárias da política pública que o Decreto nº 8.538/2015 busca alcançar.

12.3. Condições de participação:

12.3.1. 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.

12.4. Condições de habilitação:

12.5. 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:

12.6. Habilitação jurídica:

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

12.6.2. 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;

12.6.3. 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;

12.6.4. 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;

12.6.5. 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;

12.6.6. 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;

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

12.6.8. 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.

12.7. Regularidade fiscal de nível federal, de seguridade social e trabalhista:

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

12.7.2. 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;

12.7.3. 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.

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

12.7.5. 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;

12.7.6. Cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.

12.8. Qualificação Técnica:

12.8.1. Para efeito de qualificação técnica, a LICITANTE deve demonstrar sua aptidão e capacidade técnico-operacional para a execução do OBJETO mediante comprovação de prestação bem-sucedida de fornecimento de bens e de serviços em características e quantidades compatíveis com a presente licitação, mediante apresentação de um ou mais ATESTADO(S) DE CAPACIDADE TÉCNICA que deverão comprovar o fornecimento de, no mínimo, 3% (três por cento) do volume estimado de equipamentos para o item em disputa e com características compatíveis com o objeto da presente pretensão contratual, incluindo garantia e assistência técnica podendo considerar contratos já executados e/ou em execução.

12.8.2. A comprovação de capacidade técnica será realizada individualmente para cada item.

12.8.2.1. Para cada item, a(s) Licitante(s) deverá(ão) apresentar:

12.8.2.2. atestado(s) que se refiram a contratos já concluídos ou já decorrido no mínimo um ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior;

12.8.2.3. atestado(s) que se refiram a serviços prestados ou fornecimentos realizados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

12.8.3. A licitante deve disponibilizar, quando solicitado, todas as informações necessárias à comprovação de legitimidade do(s) atestado(s) apresentado(s).

12.9. **Qualificação Econômico-Financeira:**

12.9.1. De acordo com o previsto no Edital.

12.10. **Da Subcontratação**

12.10.1. Pela natureza, baixa complexidade e baixa diversidade de segmento de atuação no mercado do objeto, não será admitida a subcontratação do objeto licitatório.

12.11. **Da alteração subjetiva:**

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

12.11.2. A manutenção do contrato com empresas em processo de fusão, cisão ou incorporação será permitida desde que aprovada pelo órgão gestor da ata de registro de preços e que as empresas envolvidas apresentem e mantenham documentação habilitatória regular e plena condição de atendimento às necessidades técnicas e de documentação exigidas neste Termo de Referência.

12.12. **Matriz de risco:**

12.12.1. A presente contratação não prevê **Matriz de Riscos.**

13. **ANEXOS**

13.1. Os seguintes anexos integram este Termo de Referência:

13.1.1. Anexo I - Ordem de Serviço ou de Fornecimento de Bens - (Documento SEI nº [33736753](#));

13.1.2. Anexo II - Termo de Recebimento Provisório (Documento SEI nº [33737176](#));

13.1.3. Anexo III - Termo de Recebimento Definitivo (Documento SEI nº [33737302](#));

14. **VERSÃO DO DOCUMENTO**

Versão	Data	Descrição	Responsável
1.0	17/10/2023	Criação inicial pela EPC	EPC
2.0	13/11/2023	Ajustes	EPC

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

15.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 239, de 27 de março de 2023.

15.2. 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.

(Assinatura eletrônica) Marcone Edson da Silva Gomes Técnico em Informática Chefe da Unidade de Infraestrutura, Suporte e Segurança da Tecnologia da Informação Matrícula/SIAPE: ***4422 Integrante Técnico da EPC	(Assinatura eletrônica) Rodrigo Andrade Lima de Araújo <i>Analista de Tecnologia da Informação</i> Matrícula/SIAPE: 157*** Integrante Técnico da EPC	(Assinatura eletrônica) Eduardo Henrique Perylo de Albuquerque e Mello Souza Assistente administrativo Matrícula/SIAPE: 219 *** Integrante Administrativo da EPC
---	--	---

Aprovo o presente Termo de Referência,

Autoridade Máxima da Área de TIC
(Assinatura eletrônica) Samyr Santos Delfino Analista de TI Matrícula/SIAPE: ***7673 Chefe do Setor de Tecnologia da Informação e Saúde Digital HULW-UFPA

Aprovo o presente Termo de Referência,

Autoridade Máxima do HULW-UFPA
(Assinatura eletrônica) Marcelo Paulo Tissiani Matrícula/SIAPE: ***3498 Superintendente HULW-UFPA



Documento assinado eletronicamente por **Rodrigo Andrade Lima de Araujo, Analista de Tecnologia da Informação**, em 16/11/2023, às 06:26, 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 **Marcone Edson da Silva Gomes, Chefe de Unidade**, em 16/11/2023, às 08:42, 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 **Eduardo Henrique Perylo de Albuquerque e Mello Souza, Assistente Administrativo**, em 16/11/2023, às 16:47, 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 **Samyr Santos Delfino, Chefe de Setor**, em 22/11/2023, às 12:06, 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 **Marcelo Paulo Tissiani, Superintendente**, em 23/11/2023, às 14:18, 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 **34334466** e o código CRC **5E4317C7**.

Referência: Processo nº 23539.012015/2023-42 SEI nº 34334466

Criado por [marcone.gomes](#), versão 2 por [rodrigo.andrade](#) em 16/11/2023 06:25:27.