Governo do Estado do Rio de Janeiro

Universidade do Estado do Rio de Janeiro

Hospital Universitário Pedro Ernesto

TERMO DE REFERÊNCIA

1 - DO OBJETO:

Contratação de empresa especializada para o fornecimento de **solução integrada de segurança de perímetro de rede Fortinet**, compreendendo **02 (dois) appliances FortiGate 200G**, configurados em Alta Disponibilidade (High Availability - HA), **01 (uma) solução virtual FortiAnalyzer VM para gerenciamento centralizado de logs e eventos de segurança**, **06 (seis) transceptores ópticos SFP+ 10Gb SR**, licenciamento, subscrições de segurança, suporte técnico especializado e garantia do fabricante pelo período de **60 (sessenta) meses**, bem como os serviços de instalação, configuração, migração do ambiente existente, testes, documentação técnica e treinamento operacional, visando atender às necessidades do Hospital Universitário Pedro Ernesto - HUPE, conforme condições, quantidades e especificações estabelecidas neste Termo de Referência e seus anexos.

1.2. Justificativa da contratação

1.2.1. Até o ano de 2015, o Hospital Universitário Pedro Ernesto (HUPE) utilizava soluções de firewall baseadas em software livre (open source) para proteção de sua rede. Embora tais soluções atendessem parcialmente às necessidades à época, apresentavam limitações relevantes, tais como elevada complexidade de administração, necessidade de intervenções manuais frequentes, ausência de suporte especializado e restrições quanto à implementação de mecanismos avançados de segurança.

1.2.2. Com a evolução das ameaças cibernéticas e o aumento do volume de acessos à rede institucional, tais soluções tornaram-se insuficientes para garantir níveis adequados de proteção. Nesse contexto, a partir de 2015, foi realizada a adoção de solução do tipo UTM (Unified Threat Management), proporcionando maior capacidade de inspeção de tráfego, prevenção de intrusões, segmentação de rede e gerenciamento centralizado da segurança.

1.2.3. Entretanto, a solução atualmente em uso possui término de suporte previsto para dezembro de 2026, o que implicará na descontinuidade de atualizações, correções de vulnerabilidades e suporte técnico especializado. A manutenção de equipamentos de segurança sem suporte ativo representa risco elevado à integridade, disponibilidade e confidencialidade dos dados institucionais, bem como à continuidade dos serviços de Tecnologia da Informação e Comunicação (TIC).

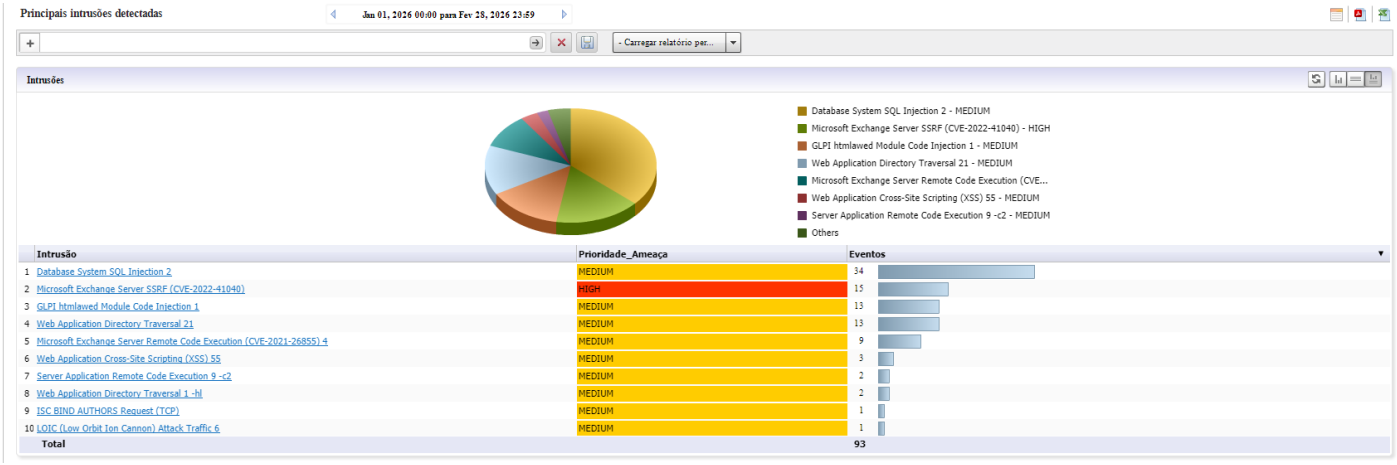
1.2.4. Adicionalmente, verifica-se que o equipamento atualmente em operação vem apresentando limitações de desempenho frente ao crescimento da demanda institucional. Observa-se aumento significativo na utilização da rede, tanto cabeada quanto sem fio, com média diária de aproximadamente 2.000 (dois mil) usuários conectados à rede Wi-Fi, esse cenário tem impactado diretamente o desempenho do appliance de firewall, especialmente em relação ao processamento de funcionalidades avançadas de segurança, como a inspeção profunda de pacotes (Deep Packet Inspection - DPI), resultando em elevada utilização de CPU e potencial degradação da performance da rede.

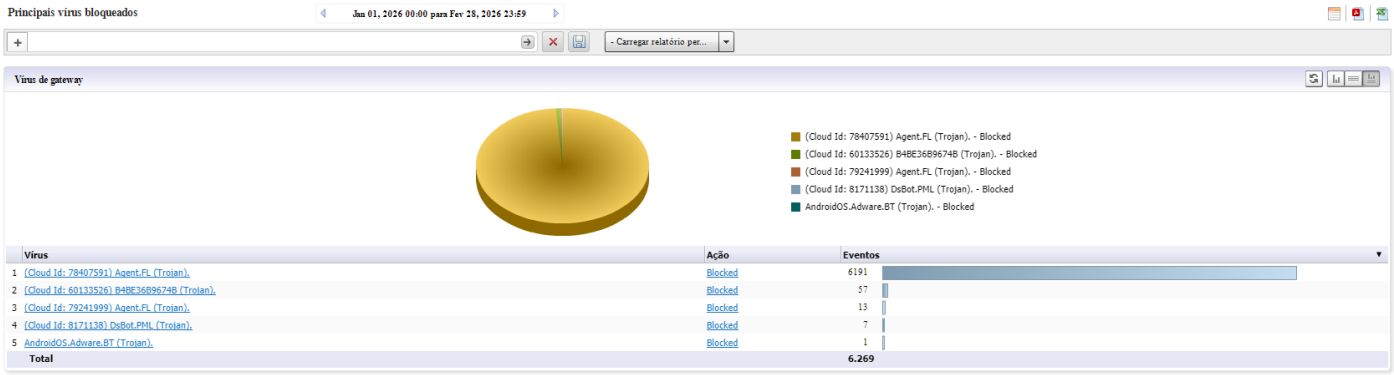
1.2.5. Tal limitação compromete a eficiência dos mecanismos de segurança implementados, podendo ocasionar lentidão no tráfego, indisponibilidade de serviços e até mesmo falhas na detecção e mitigação de ameaças cibernéticas.

1.2.6. O HUPE é uma instituição de referência na assistência à saúde, sendo responsável pelo atendimento de grande volume de pacientes e pelo tratamento de dados pessoais e dados pessoais sensíveis. Nesse contexto, a proteção desses dados é essencial, inclusive para atendimento às disposições da Lei Geral de Proteção de Dados Pessoais (LGPD).

1.2.7. Adicionalmente, o cenário atual evidencia o aumento significativo de ataques cibernéticos direcionados a instituições de saúde, incluindo eventos recentes que resultaram na indisponibilidade de sistemas e comprometimento de dados em organizações públicas e privadas. Tais ocorrências reforçam a necessidade de adoção de soluções robustas e atualizadas de segurança da informação.

1.2.8. Corroborando esse contexto, relatórios extraídos da solução atualmente em uso no HUPE, no período correspondente aos meses de janeiro e fevereiro do corrente ano, demonstram a ocorrência contínua de tentativas de intrusão e outros eventos de segurança, evidenciando a exposição do ambiente a ameaças cibernéticas e a necessidade de mecanismos mais modernos e eficazes de proteção.





1.2.9. Diante do exposto, justifica-se a necessidade de contratação de nova solução de firewall, com recursos avançados de segurança, gerenciamento centralizado e suporte técnico especializado, de forma a assegurar a proteção da infraestrutura de TIC, a continuidade dos serviços assistenciais e administrativos e a mitigação de riscos relacionados à segurança da informação.

1.3. Da Necessidade de Padronização e Compatibilidade (Art. 41, inciso I, alíneas "a", "b" e "d" da Lei nº 14.133/2021, c/c art. 19 do Decreto Estadual nº 48.816/2023)

1.3.1. A presente contratação observa a política institucional de padronização tecnológica da Universidade do Estado do Rio de Janeiro - UERJ, definida e coordenada pela Diretoria-Geral de Tecnologia da Informação - DGTI, com fundamento no art. 41, inciso I, alíneas "a", "b" e "d", da Lei nº 14.133/2021, c/c o art. 19 do Decreto Estadual nº 48.816/2023.

1.3.2. A solução especificada neste Termo de Referência integra o ecossistema Fortinet já adotado pela UERJ em diversas unidades acadêmicas, administrativas e hospitalares, permitindo a manutenção da compatibilidade técnica, da interoperabilidade entre os ativos existentes, do

gerenciamento centralizado e da continuidade operacional da infraestrutura institucional de segurança da informação.

1.3.3. A utilização da mesma plataforma tecnológica reduz riscos de incompatibilidade, simplifica as atividades de administração, suporte e manutenção, possibilita a aplicação uniforme das políticas de segurança, otimiza os processos de atualização de firmware e assinaturas de segurança e preserva a integração nativa entre os appliances FortiGate e a solução de gerenciamento centralizado FortiAnalyzer.

1.3.4. A padronização também contribui para a racionalização dos custos operacionais, reduz a necessidade de capacitação em múltiplas plataformas, facilita a expansão futura da infraestrutura tecnológica e minimiza os riscos inerentes à migração para soluções de fabricantes distintos, especialmente em ambiente hospitalar, onde a indisponibilidade dos serviços pode impactar diretamente a assistência à saúde.

1.3.5. A motivação técnica detalhada para a adoção da plataforma Fortinet, bem como a demonstração da padronização institucional, da compatibilidade tecnológica e da vantajosidade da solução, encontram-se devidamente desenvolvidas no Estudo Técnico Preliminar que integra a fase preparatória da presente contratação, incluindo o histórico das contratações anteriormente realizadas pela UERJ (Processos E-26/007/7210/2019, SEI-260007/034118/2021 e SEI-260006/047118/2024).

1.4. Instrumentos de planejamento

1.4.1.A presente demanda encontra-se prevista no **Plano de Contratações Anual - PCA/2026** deste órgão, elaborado nos termos do Decreto Estadual nº 48.760, de 23 de outubro de 2023, que dispõe sobre o PCA no âmbito da Administração Pública Estadual Direta, Autárquica e Fundacional do Estado do Rio de Janeiro.

1.4.2. Os itens estão registrados no PCA/2026 sob os **IDs nº 18817, 18820 e 18821** disponível para consulta no Portal Nacional de Contratações Públicas - PNCP, no endereço: https://pncp.gov.br/app/pca/42498600000171/2026/5.

1.5. Disponibilidade Orçamentária e Financeira

As despesas com a execução do presente contrato correrão à conta das seguintes dotações orçamentárias, para o corrente exercício de 2026.
Unidade Orçamentária (UO) - HUPE:404340
Fonte de Recursos (FR) - HUPE: 122
Natureza da Despesa (ND): 4.4.90.52 - Equipamentos e Material Permanente e 3.3.90.40 Serviços de TIC.

1.6. Classificação dos bens ou serviços da contratação

1.6.1. Os itens que compõem o objeto desta contratação possuem características padronizadas e usuais de mercado, com especificações de desempenho e qualidade objetivamente definidas por meio de padrões técnicos amplamente difundidos no segmento de Tecnologia da Informação e Comunicação - TIC, enquadrando-se, portanto, como **bens comuns**, nos termos do art. 6º, inciso XIII, da Lei nº 14.133/2021.

1.6.2. A solução é composta pelo fornecimento de appliances de firewall de próxima geração (NGFW), solução de gerenciamento centralizado de logs e eventos, licenciamento, suporte técnico, garantia do fabricante, transceivers e demais componentes necessários à sua plena operação, bem

como pelos serviços acessórios de instalação, configuração, migração, testes e treinamento operacional.

1.6.3. Embora contemple serviços associados, estes possuem natureza acessória e complementar ao fornecimento da solução, sendo indispensáveis para sua correta implantação e funcionamento, não descaracterizando a predominância do fornecimento de bens.

1.6.4. Dessa forma, a contratação caracteriza-se como **aquisição de bens comuns de Tecnologia da Informação e Comunicação - TIC, com prestação de serviços acessórios especializados**, a ser processada por meio de licitação na modalidade Pregão, em sua forma eletrônica, nos termos da legislação vigente.

2 - DESCRIÇÃO DO OBJETO:

2.1. Definição do objeto

2.1.1. Constitui objeto da presente contratação o fornecimento de solução integrada de segurança de perímetro de rede, composta por **appliances FortiGate 200G** operando em Alta Disponibilidade (High Availability - HA), **solução de gerenciamento centralizado de logs FortiAnalyzer VM**, módulos transceptores ópticos SFP+ 10Gb compatíveis, licenciamento, subscrições de segurança, suporte técnico especializado e garantia do fabricante pelo período de 60 (sessenta) meses, bem como serviços especializados de instalação, configuração, configuração, migração, testes, documentação e treinamento operacional, conforme especificações constantes deste Termo de Referência.

2.1.2. A solução deverá ser fornecida de forma integrada e plenamente compatível com a infraestrutura tecnológica atualmente utilizada no âmbito da Universidade do Estado do Rio de Janeiro - UERJ, observando a política institucional de padronização tecnológica, a interoperabilidade com o ambiente Fortinet existente, a continuidade operacional, a segurança da informação, a alta disponibilidade dos serviços e o gerenciamento centralizado dos ativos de segurança de rede.

2.1.3. A contratação tem por finalidade substituir a atual infraestrutura de firewall do Hospital Universitário Pedro Ernesto - HUPE por solução corporativa de última geração, ampliando a capacidade de prevenção, detecção e resposta a ameaças cibernéticas, assegurando maior disponibilidade dos serviços institucionais, proteção dos dados pessoais sensíveis tratados pela instituição e conformidade com os requisitos de segurança da informação e da Lei Geral de Proteção de Dados - LGPD.

2.2. Disposições Gerais

2.2.1. Todos os equipamentos, softwares, licenças, subscrições, acessórios e componentes que integram a solução deverão ser novos, sem uso anterior, em linha de fabricação e comercialização pelo fabricante na data da entrega, não sendo admitidos equipamentos recondicionados, remanufaturados, descontinuados ou destinados exclusivamente a programas de demonstração.

2.2.2. A solução deverá ser fornecida com todas as licenças, assinaturas, subscrições, atualizações, firmwares, softwares e demais componentes necessários ao pleno funcionamento das funcionalidades especificadas neste Termo de Referência durante todo o período de vigência contratual.

2.2.3. Os equipamentos deverão ser entregues acompanhados de todos os cabos, conectores, módulos, transceivers, fontes, kits de montagem em rack, manuais, acessórios e demais componentes necessários à sua instalação e operação, sem ônus adicional para a CONTRATANTE.

2.2.4. Todos os componentes da solução deverão possuir compatibilidade plena entre si, garantindo seu funcionamento integrado e observando as melhores práticas de segurança da informação, disponibilidade e desempenho.

2.2.5. A CONTRATADA será responsável pela instalação, configuração, migração do ambiente existente, testes operacionais, documentação da solução implantada e transferência de conhecimento à equipe técnica do HUPE, observadas as condições estabelecidas neste Termo de Referência.

2.2.6. O suporte técnico e a garantia deverão ser prestados pelo fabricante ou por empresa por ele autorizada, abrangendo atualização de versões, correções de falhas, substituição de componentes defeituosos e demais serviços necessários à manutenção da solução em pleno funcionamento durante todo o período contratado.

2.2.7. Todos os equipamentos e licenças fornecidos deverão ser registrados em nome da Universidade do Estado do Rio de Janeiro - UERJ, possibilitando à CONTRATANTE acesso aos portais de suporte, documentação técnica, atualizações e demais recursos disponibilizados pelo fabricante.

2.2.8. A solução deverá atender integralmente aos requisitos técnicos, operacionais, de segurança e de desempenho estabelecidos neste Termo de Referência.

2.3. Requisitos de Negócio

2.3.1. A solução deverá prover mecanismos de proteção do perímetro de rede do HUPE, garantindo a segurança, disponibilidade, integridade e confidencialidade das informações trafegadas pelos ambientes institucionais.

2.3.2. A solução deverá possibilitar a implementação, gerenciamento e fiscalização centralizada das políticas de segurança da informação aplicáveis aos ambientes administrativos, acadêmicos, assistenciais e de pesquisa da instituição.

2.3.3. A solução deverá suportar o crescimento da infraestrutura tecnológica do HUPE durante o período contratual, garantindo capacidade operacional compatível com a evolução dos serviços digitais e das demandas institucionais.

2.3.4. A solução deverá permitir a continuidade dos serviços de rede e segurança da informação, minimizando riscos de indisponibilidade decorrentes de falhas de hardware, software ou eventos de segurança cibernética.

2.3.5. A solução deverá possibilitar a geração, armazenamento, pesquisa e correlação de registros (logs) de eventos de segurança, contribuindo para atividades de auditoria, monitoramento, rastreabilidade e resposta a incidentes.

2.3.6. A solução deverá ser compatível com o padrão tecnológico adotado pela Universidade do Estado do Rio de Janeiro - UERJ, observando os requisitos de padronização, interoperabilidade, integração e continuidade operacional definidos institucionalmente.

2.3.7. A solução deverá permitir administração, monitoramento e suporte compatíveis com a estrutura operacional da equipe técnica do HUPE, reduzindo riscos operacionais e facilitando a sustentação do ambiente ao longo de seu ciclo de vida.

2.3.8. A contratação deverá contemplar transferência de conhecimento à equipe técnica da CONTRATANTE, mediante treinamento e documentação, visando garantir autonomia operacional e adequada gestão da solução implantada.

2.3.9. A solução deverá atender às necessidades de proteção dos ativos de Tecnologia da Informação e Comunicação do HUPE, contribuindo para a continuidade dos serviços essenciais prestados à assistência, ensino, pesquisa e gestão hospitalar.

2.4. Requisitos de Manutenção

2.4.1. Todas as rotinas de manutenção necessárias ao pleno e adequado funcionamento da solução ao longo da vigência contratual serão de responsabilidade da CONTRATADA.

2.4.2. A CONTRATADA deverá disponibilizar canal de atendimento por meio de aplicação web, número de telefone ou endereço eletrônico para abertura e acompanhamento de chamados técnicos e esclarecimento de dúvidas, em regime de 24 horas por dia, 7 dias por semana, durante todos os dias do ano, inclusive sábados, domingos e feriados;

2.4.3. Não há outros requisitos temporais de manutenção a serem considerados além do cronograma de entrega e implantação previsto nas condições gerais desta contratação.

2.5. Requisitos Tecnologicos

2.5.1. De projeto e de implementação

2.5.1.1. Antes do início das atividades de implantação, a CONTRATADA deverá realizar, nas dependências do HUPE ou em ambiente acordado entre as partes, **reunião inicial de projeto (kick-off)** envolvendo as equipes técnicas de TI, com o objetivo de definir o Plano de Trabalho de instalação e configuração da solução.

2.5.1.2. Após a reunião de kick-off, a CONTRATADA deverá elaborar e entregar à HUPE o **Projeto Executivo**, contemplando: planejamento e escopo do projeto, cronograma de execução, discriminação dos entregáveis, dimensionamento da infraestrutura necessária, composição da equipe técnica com perfis e quantitativos.

2.5.1.3. A etapa de instalação e configuração compreenderá: a instalação física dos appliances e do gerenciamento de logs no ambiente do HUPE, a configuração do cluster HA ativo-passivo, a migração das políticas, regras e configurações de firewall eventualmente vigentes no ambiente atual, caso haja viabilidade técnica e a integração para coleta e correlação de logs.

2.5.1.4. A instalação deverá ocorrer de forma gradual e transparente, conforme a conveniência operacional do HUPE, podendo as atividades ser executadas em horário comercial, período noturno ou final de semana, conforme necessidade definida pela Administração. Durante toda a etapa, a equipe técnica da CONTRATADA deverá estar presente nos horários de testes, implantação e migração definidos pelo HUPE.

2.5.1.5. A CONTRATADA deverá planejar e executar a instalação com total interoperabilidade no ambiente atual, sem impacto no ambiente de produção hospitalar. Para tanto, deverá disponibilizar ferramentas ou scripts que permitam o retorno imediato ao estado original da infraestrutura caso a implantação apresente falha. Todas as licenças necessárias ao pleno funcionamento do ambiente de produção deverão ser fornecidas pela CONTRATADA sem ônus adicional.

2.5.1.6. O encaminhamento formal de cada demanda ocorrerá por meio de emissão de **Ordem de Serviço/Fornecimento**, e quaisquer mudanças nos métodos executivos que fujam às especificações acordadas deverão ser submetidas previamente, por escrito, à aprovação da equipe de TI.

2.5.2. Do suporte técnico

2.5.2.1. A CONTRATADA deverá disponibilizar, por meio de portal web com autenticação por login e senha para usuários autorizados do HUPE, sistema de registro e acompanhamento de chamados de suporte técnico, em regime **24x7x365** (vinte e quatro horas por dia, todos os dias do ano, inclusive sábados, domingos e feriados), considerada a criticidade do ambiente hospitalar.

2.5.2.2. A CONTRATANTE poderá abrir número ilimitado de chamados durante a vigência da garantia. Entende-se por suporte técnico a prestação de informações, orientações, configurações, instalações, atualizações e reparos necessários ao bom funcionamento da solução, incluindo intervenção direta nos equipamentos sempre que necessário.

2.5.2.3. Durante o atendimento, a CONTRATADA poderá analisar a solução, seus logs de sistema e sugerir melhorias de configuração, cabendo à equipe técnica do HUPE a decisão sobre a aplicação das recomendações.

2.5.2.4. Os prazos de atendimento do suporte técnico deverão observar os seguintes níveis de severidade:

Severidade	Descrição	1º Contato	Solução
Urgente	Solução totalmente inoperante	até 30 minutos	até 2 horas
Importante	Solução parcialmente inoperante, com necessidade de interrupção	até 1 hora	até 4 horas

Normal	Problema de funcionamento sem necessidade de interrupção	até 2 hora	até 24 horas
Informação	Dúvidas e solicitações diversas	até 8 hora	até 48 horas

2.5.2.5. A severidade poderá ser reavaliada quando verificado enquadramento incorreto, passando a vigorar os novos prazos a partir da reavaliação. A CONTRATADA poderá solicitar prorrogação de prazo antes do seu vencimento, devidamente justificada, cabendo à CONTRATANTE aceitar ou não o pedido. Todos os prazos serão contados a partir da abertura do chamado, independentemente do canal utilizado.

2.5.3. Da garantia do produto

2.5.3.1. Considera-se garantia a obrigação da CONTRATADA de reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, os equipamentos e componentes em que se verificarem vícios, defeitos ou incorreções durante o prazo contratual. A garantia deverá prover, sem ônus adicionais ao HUPE:

- Acesso para download de patches, drivers e demais atualizações de software necessárias, disponíveis no portal do fabricante durante todo o período de garantia;
- Disponibilização das revisões de manuais técnicos e documentação dos equipamentos adquiridos.

2.5.4. De metodologia de trabalho

2.5.4.1. São instrumentos formais de comunicação entre o HUPE e a CONTRATADA no âmbito desta contratação:

- Ordem de Serviço/Fornecimento;
- Plano de Inserção/Projeto Executivo;
- Termos de Recebimento Provisório e Definitivo;
- Chamado registrado na Central de Atendimento/Suporte da CONTRATADA ;
- Ofícios;
- Relatórios e Atas de Reunião;
- Comunicações por e-mail institucional;
- Demais termos previstos no instrumento convocatório.

2.5.4.2. Toda comunicação formal entre as partes ocorrerá por intermédio do preposto designado pela CONTRATADA , ou seu substituto. O acionamento da Central de Suporte poderá ser realizado por meio de chamado via telefone com registro de protocolo ou por sistema informatizado que permita o registro formal da demanda e seu rastreamento.

2.5.5. Horário de funcionamento e de prestação dos serviços

2.5.5.1. O horário regular de funcionamento do HUPE é das **09h às 18h, de segunda a sexta-feira**. Ressalvam-se eventuais emergências, cuja ocorrência pode dar-se em qualquer horário e dia da semana, razão pela qual o suporte técnico deverá estar disponível em regime 24x7x365, conforme estabelecido na alínea "b" acima.

2.5.5.2. O acesso de representante da CONTRATADA às dependências do hospital deverá ocorrer mediante **prévia comunicação entre as partes**, utilizando os mecanismos formais de comunicação definidos neste instrumento, observadas as normas de controle de acesso e segurança institucional vigentes no HUPE.

2.6. Requisitos de Segurança da Informação, Sigilo E Lgpd

2.6.1. A execução contratual deverá observar a Política de Segurança da Informação do HUPE, a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais, o Decreto Estadual nº 48.891/2024 e demais normas aplicáveis à segurança da informação, privacidade, sigilo e proteção de dados. A CONTRATADA deverá manter sigilo absoluto sobre topologias, endereços, regras, configurações, logs, relatórios, credenciais, incidentes, vulnerabilidades, diagramas e quaisquer informações obtidas em razão da execução contratual.

2.6.2. A CONTRATADA deverá utilizar os dados e informações acessados exclusivamente para as finalidades necessárias à execução contratual, sendo vedada sua reprodução, compartilhamento, divulgação, transferência ou utilização para finalidade diversa, salvo autorização expressa da CONTRATANTE ou obrigação legal. Deverá, ainda, orientar seus profissionais quanto aos deveres de sigilo e proteção de dados, exigindo assinatura de termos de confidencialidade e responsabilidade quando previsto no Termo de Referência.

2.6.3. A CONTRATADA deverá comunicar imediatamente ao fiscal do contrato qualquer incidente de segurança, acesso indevido, exposição de dados, perda, alteração, destruição, comunicação ou tratamento inadequado de informações, adotando medidas de contenção, documentação e cooperação com a CONTRATANTE. O tratamento de logs, configurações e informações sensíveis deverá observar controle de acesso, rastreabilidade, princípio do menor privilégio e preservação de evidências.

2.7. Características gerais da solução

2.7.1. Características gerais da solução NGFW

2.7.1.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall - NGFW, com serviço de firewall stateful nativo, não sendo permitidas soluções em appliance virtual, open source ou baseadas em computadores de uso geral para o item de firewall físico.
2.7.1.2. Por funcionalidades de NGFW, entende-se, no mínimo, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões, com otimização para análise de conteúdo de aplicações em camada 7.
2.7.1.3. O equipamento deverá ser fornecido com acessórios necessários para instalação em rack padrão 19 polegadas, incluindo bandejas, suportes, trilhos ou componentes equivalentes, quando aplicáveis ao modelo ofertado.
2.7.1.4. A solução deverá suportar acesso administrativo seguro por HTTPS, SSH e API, observadas as políticas internas de segurança da informação do HUPE.
2.7.1.5. O dispositivo de proteção de rede deve possuir suporte a VLANs, subinterfaces Ethernet lógicas, roteamento estático e dinâmico, incluindo, no mínimo, BGP e OSPF, além de DHCP Relay e DHCP Server.
2.7.1.6. Deve permitir NAT dinâmico, NAT estático, PAT, NAT de origem, NAT de destino, aplicação simultânea de NAT de origem e destino, bem como recursos equivalentes de tradução para IPv6 quando suportados pelo fabricante.
2.7.1.7. Deve permitir monitoramento via SNMP do uso de CPU, memória, armazenamento, VPN, cluster, interfaces e eventos de segurança, bem como envio de logs para sistemas externos de monitoramento e análise.
2.7.1.8. A solução deve possuir proteção anti-spoofing, operar em modo Camada 3 para inspeção de dados em linha e suportar controle, inspeção e descriptografia SSL/TLS conforme política autorizada pela Administração.
2.7.1.9. A solução deve suportar configuração de alta disponibilidade nos modos ativo/passivo e ativo/ativo, com sincronização de sessões e configurações, incluindo políticas de firewall, NAT, objetos, VPNs e tabelas de encaminhamento, quando aplicável.

2.7.1.10. Os equipamentos fornecidos deverão pertencer à solução ofertada ou possuir interoperabilidade oficialmente comprovada pelo fabricante, assegurando padronização, compatibilidade funcional e suporte integral aos recursos exigidos.
2.7.1.11. O equipamento deverá ser novo, de primeiro uso e, na data da apresentação da proposta, não poderá constar, no portal oficial do fabricante, como descontinuado, em processo de descontinuação, end-of-sale - EOS ou end-of-life - EOL.
2.7.1.12. O equipamento deverá possuir arquitetura de hardware com aceleração integrada para tratamento de fluxos de rede, segurança e inspeção de conteúdo, de modo a assegurar desempenho adequado em funções de inspeção profunda e criptografia.

2.7.2. Características específicas da Solução NGFW
2.7.2.1. Deve possuir throughput mínimo de 6 Gbps com as funcionalidades de Controle de Aplicações, IPS (Intrusion Prevention System), Antivírus e Antispyware habilitadas simultaneamente. Caso o fabricante divulgue múltiplos números de desempenho para essas funcionalidades, será considerado o menor valor informado.
2.7.2.2. Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 35 Gbps.
2.7.2.3. Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 30 Gbps.
2.7.2.4. Deve permitir, no mínimo, 5.000.000 conexões simultâneas.
2.7.2.5. Deve permitir, no mínimo, 350.000 novas conexões por segundo.
2.7.2.6. Deve suportar, no mínimo, 4.000 políticas de firewall..
2.7.2.7. Deve permitir, e estar licenciado para a utilização de 1000 túneis VPN site-to-site simultâneos.
2.7.2.8. Deve permitir, e estar licenciado para a utilização de 10.000 túneis VPN client-to-site simultâneos.
2.7.2.9. Deve suportar instalação em rack padrão EIA-310 de 19 polegadas, acompanhado de todos os acessórios necessários para montagem.
2.7.2.10. O appliance deverá possuir, no mínimo, 8 interfaces RJ-45 Gigabit Ethernet.
2.7.2.11. O appliance deverá possuir, no mínimo, 4 interfaces SFP GE para conexão por fibra óptica.
2.7.2.12. O appliance deverá possuir, no mínimo, 8 interfaces SFP+ de 10 Gigabit Ethernet para conexão por fibra óptica.
2.7.2.13. Deve suportar inspeção SSL/TLS (SSL Inspection) com desempenho mínimo de 6 Gbps.
2.7.2.14. Deve suportar throughput mínimo de 8 Gbps para sistema de prevenção de intrusão (IPS).
2.7.2.15. Deve suportar configuração em alta disponibilidade (HA), nos modos Active-Active e Active-Passive.

2.7.3. Políticas de segurança e controle
2.7.3.1. Suportar controles por zonas de segurança, portas, protocolos, aplicações, grupos de aplicações, usuários, grupos de usuários, IPs, redes e geolocalização.
2.7.3.2. Suportar controle, inspeção e descriptografia SSL/TLS por política para tráfego de saída, inclusive conexões negociadas com TLS 1.2 e TLS 1.3, quando permitido pela política institucional.
2.7.3.3. Permitir bloqueio de arquivos por extensão e identificação por tipo real de arquivo, ainda que a extensão seja alterada.
2.7.3.4. Suportar objetos e regras IPv4, IPv6 e multicast, com agendamento de políticas para ativação e desativação automática em horários definidos.
2.7.3.5. Permitir criação de políticas por aplicação sem necessidade de liberação isolada de portas e protocolos, com atualização automática da base de assinaturas de aplicações.

2.7.4. SD-WAN, roteamento e QoS
2.7.4.1. Prover recursos de roteamento inteligente, definindo o melhor caminho para uma aplicação com base em regras e métricas configuráveis.
2.7.4.2. Permitir políticas baseadas em IP de origem/destino, VLAN, porta, domínio, URL, grupos de usuários e aplicação em camada 7.
2.7.4.3. Monitorar falhas por health check, incluindo ping, HTTP, TCP/UDP echo, DNS, TCP-connect, TWAMP ou equivalentes.
2.7.4.4. Permitir balanceamento de tráfego entre múltiplos links, escolha por menor custo, melhor qualidade, peso, hash ou política equivalente.

2.7.4.5. Permitir roteamento baseado em latência, jitter, perda de pacotes, banda ocupada e critérios combinados.
2.7.4.6. Implementar QoS/traffic shaping com banda mínima, banda máxima, DSCP, filas de prioridade e agendamento de políticas.

2.7.5. Controle de aplicações e prevenção de ameaças
2.7.5.1. Reconhecer aplicações independentemente de porta e protocolo, inclusive tráfego evasivo, aplicações criptografadas e protocolos encapsulados.
2.7.5.2. Reconhecer, no mínimo, 1.700 aplicações distintas ou quantidade superior oficialmente suportada pelo fabricante.
2.7.5.3. Possuir módulos integrados de IPS, antivírus, antimalware, anti-spyware, botnet protection, filtro DNS e recursos contra ataques DoS/DDoS.
2.7.5.4. Permitir ações como permitir, registrar, bloquear, quarentenar IP de origem e aplicar perfis de segurança por regra.
2.7.5.5. Permitir mitigação de ameaças avançadas por antivírus, reputação em nuvem, sandboxing, análise dinâmica, detecção de callback ou recursos equivalentes.

2.7.6. Filtro web, identidade e VPN
2.7.6.1. Permitir criação de políticas de acesso web por URL, categoria, grupo de usuários, IP, rede, zona de segurança e agendamento.
2.7.6.1. Possuir base de categorias de URL mantida e atualizada pelo fabricante, com possibilidade de exceções e página de bloqueio customizada.
2.7.6.1. Integrar-se a Microsoft Active Directory, LDAP, RADIUS e bases locais para identificação de usuários e grupos, com suporte a SSO e portal cativo quando aplicável.
2.7.6.1. Suportar VPN IPsec site-to-site e client-to-site, com algoritmos criptográficos atuais, IKEv1/IKEv2, autenticação por certificado e interoperabilidade com fabricantes consolidados.

2.7.7. Licenciamento da Solução
2.7.7.1. Todos os appliances FortiGate deverão ser fornecidos com **licenciamento FortiGuard Enterprise Protection**, ou denominação equivalente adotada pelo fabricante para o mesmo conjunto de funcionalidades, válido pelo período de **60 (sessenta) meses**, contemplando todas as licenças, subscrições e serviços necessários ao pleno funcionamento da solução.
2.7.7.2. O licenciamento deverá compreender, no mínimo, as funcionalidades de prevenção de intrusão (IPS), proteção contra malware, controle de aplicações, filtragem Web (Web Filtering), filtragem DNS (DNS Filtering), inspeção SSL/TLS, inteligência de ameaças, reputação de endereços IP, proteção contra botnets, antivírus, antispam (quando aplicável), serviços de segurança baseados em nuvem e demais funcionalidades integrantes do bundle **Enterprise Protection** do fabricante.
2.7.7.3. Entende-se por atualização de assinaturas de proteção todas as funcionalidades, automáticas ou manuais, necessárias para manter a solução permanentemente atualizada quanto aos mecanismos de identificação e proteção contra ameaças, incluindo, mas não se limitando a, assinaturas de IPS, antivírus, controle de aplicações, filtragem Web, filtragem DNS, geolocalização, reputação de endereços IP, botnets e demais serviços disponibilizados pelo fabricante.
2.7.7.4. Todas as licenças e subscrições deverão ser registradas em nome da CONTRATANTE no portal oficial do fabricante, permanecendo ativas durante toda a vigência contratual.
2.7.7.5. Caso o fabricante altere a nomenclatura comercial do bundle **Enterprise Protection** durante a vigência do certame, será aceita a versão sucessora, desde que contemple, no mínimo, o mesmo conjunto de funcionalidades, níveis de proteção e serviços de segurança especificados neste Termo de Referência, sem ônus adicional para a CONTRATANTE.

2.7.8. Suporte do Fabricante
2.7.8.1. O suporte deverá ser oficial do fabricante, pelo prazo de 60 meses, com cobertura compatível com o nível FortiCare Premium ou superior oficialmente aplicável ao modelo ofertado.
2.7.8.2.. Deverá incluir atualizações de firmware, acesso a versões de software, atualizações de bases de IPS, antivírus, controle de aplicações, filtro web/URL/DNS e serviços de segurança contratados.

2.7.8.3. Deverá permitir abertura de chamados junto ao fabricante, atendimento 24x7, tratamento de incidentes críticos e escalonamento técnico conforme regras do nível contratado.
2.7.8.4. Deverá incluir cobertura de substituição de hardware/RMA nos termos do nível contratado, sem ônus adicional à Administração durante o período de cobertura.
2.7.8.5. A comprovação deverá ocorrer por registro dos números de série no portal oficial do fabricante, com suporte ativo e vinculado ao HUPE ou conforme orientação formal do HUPE.

2.7.9. Características do Gerenciamento de Logs
2.7.9.1. A solução deverá operar como appliance virtual, compatível com hipervisores corporativos amplamente utilizados, incluindo VMware ESXi, Microsoft Hyper-V e KVM, conforme documentação oficial vigente.
2.7.9.2. Deverá suportar ingestão mínima de 50 GB de logs por dia e receber/processar logs dos dispositivos NGFW contemplados na contratação.
2.7.9.3. Deverá permitir gerenciamento por interface Web segura e acesso administrativo controlado, com perfis de acesso, segregação de permissões, autenticação LDAP/RADIUS/TACACS+ ou equivalente.
2.7.9.4. Deverá permitir armazenamento, visualização, pesquisa, exportação, encaminhamento e auditoria de logs, incluindo suporte a Syslog e CEF ou formatos equivalentes.
2.7.9.5. Deverá possuir painéis, relatórios, alertas, correlação de eventos, automação de segurança e recursos de investigação compatíveis com o ecossistema Fortinet.
2.7.9.6. A CONTRATANTE disponibilizará a infraestrutura de virtualização, cabendo à CONTRATADA informar formalmente os requisitos mínimos de vCPU, memória, armazenamento, IOPS, rede e demais dependências técnicas.
2.7.9.7. A solução deverá estar licenciada e com suporte ativo pelo prazo de 60 meses, incluindo atualizações, suporte técnico do fabricante e manutenção das funcionalidades CONTRATADA s.
2.7.9.8. A solução deverá ser dimensionada para retenção mínima de logs de 12 meses, desde que a infraestrutura de armazenamento disponibilizada pela CONTRATANTE atenda aos requisitos informados pela CONTRATADA e validados pela fiscalização técnica.

2.7.10. Características dos módulos transceptores óptico
2.7.10.1. Os módulos ópticos deverão ser originais Fortinet ou oficialmente homologados/compatíveis com a solução Fortinet ofertada, com comprovação por documentação técnica ou matriz de compatibilidade.
2.7.10.2. Não serão aceitos transceivers sem comprovação de compatibilidade, sem identificação de part number, sem origem regular ou que comprometam o suporte oficial da solução.

2.7.11. Requisitos de Capacitação
2.7.11.1. O treinamento operacional compõe o escopo da contratação e deverá observar as seguintes condições:
2.7.11.1. O treinamento será voltado à equipe técnica de TI do HUPE, com foco na operacionalização da solução em cluster HA e do gerenciamento de log, viabilizando a transferência de conhecimento sobre recursos, configurações e rotinas de administração existentes na solução implantada;
22.7.11.1. A CONTRATADA deverá submeter à CONTRATANTE, previamente ao início das aulas, o conteúdo programático detalhado do treinamento, cabendo à Administração a prerrogativa de não aceitar módulos considerados inadequados, podendo solicitar substituição de instrutor ou repetição de conteúdo;
2.7.11.1. O treinamento deverá ser ministrado por profissional devidamente certificado pelo fabricante, com comprovação por meio de certificados ou declaração oficial emitida pelo fabricante, em nível compatível com os equipamentos objeto desta contratação;
2.7.11.1. Deverá ser fornecido certificado de conclusão para cada participante ao término do treinamento;
2.7.11.1. O conteúdo mínimo deverá abranger: instalação, configuração, operação e gerenciamento da solução, operação do cluster HA, geração de relatórios e análise de eventos de segurança, resolução de problemas, e atualização de assinaturas e licenças. O treinamento deverá incluir laboratórios práticos realizados na mesma versão dos produtos efetivamente fornecidos;
2.7.11.1. A carga horária mínima deverá ser de 40 (quarenta) horas, devendo ser realizado em dias

úteis, sem exceder o horário comercial, com início no prazo máximo de 20 (vinte) dias úteis contados da emissão da Ordem de Serviço;
2.7.11.1. O treinamento será realizado em língua portuguesa, na modalidade presencial ou remota, com todos os materiais didáticos e audiovisuais fornecidos pela CONTRATADA , sem custos adicionais à Administração.

2.8. Identificação dos itens, quantidades e unidades

2.8.1. A presente contratação será composta pelos itens descritos na tabela de quantitativos deste Termo de Referência, contemplando o fornecimento de solução integrada de segurança de perímetro de rede, incluindo appliances de firewall de próxima geração (NGFW), solução de gerenciamento centralizado de logs e eventos, transceivers ópticos e treinamento operacional.

2.8.2. Os itens que compõem o objeto possuem relação de complementaridade e interdependência técnica, sendo destinados à implantação de uma solução única e integrada de segurança da informação para o ambiente computacional do Hospital Universitário Pedro Ernesto - HUPE.

2.8.3. Os quantitativos foram definidos com base nas necessidades operacionais da infraestrutura tecnológica do HUPE, observando os requisitos de disponibilidade, desempenho, segurança, capacidade de expansão e continuidade dos serviços institucionais.

2.8.4. A identificação dos itens, respectivas quantidades e unidades de fornecimento encontra-se detalhada na tabela constante deste Termo de Referência.

Quadro 1 - Quantidade Estimada do Registro de Preços

LOTE 1						
ITEM	**ID PCA**	**CÓD. ITEM**	**ID SIGA**	**ESPECIFICAÇÕES**	**UND. FORNECIMENTO**	**QUANTIDADE**
1	18817	7060.012.0023	168257	APPLIANCE FIREWALL - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES (FORTIGATE 200G - ENTERPRISE PROTECTION + FORTICARE PREMIUM)	UNIDADE	2
2	18820	7011.005.0045	180940	CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL COM GARANTIA DE 60 MESES (FORTIANALYZER - FOR 50 GBDAY CENTRAL LOGGING & ANALYTICS INCLUDE FORTICARE PREMIUM SUPPORT IOC SECURITY AUTOMATION SERVICE AND FORTIGUARD OUTBREAK DETECTION SERVICE)	UNIDADE	1

3	-	6099.010.0046	196267	TRANSCEIVER ÓPTICO 10GE (FN-TRAN-SFP+SR)	UNIDADE	6
4	18821	0335.005.0718	180945	TREINAMENTO OPERACIONAL PARA FIREWALL	ALUNO	4

2.9. Informações Complementares

2.9.1. Os appliances de firewall deverão ser fornecidos com hardware dedicado, transceivers ópticos, licenciamento completo das funcionalidades de segurança, garantia, atualização de assinaturas, suporte técnico do fabricante, instalação, configuração e serviços necessários para entrada da solução em operação, pelo período de 60 (sessenta) meses.

2.9.2. A solução de gerenciamento centralizado deverá permitir o armazenamento, consolidação, correlação, monitoramento e análise dos logs gerados pelos appliances de firewall, possibilitando maior capacidade de auditoria, rastreabilidade, identificação de incidentes de segurança e apoio às atividades operacionais da equipe técnica.

2.9.3. A contratação também contempla treinamento operacional especializado, visando capacitar os servidores responsáveis pela administração, monitoramento e sustentação da solução, de forma a assegurar adequada utilização dos recursos tecnológicos contratados e promover autonomia operacional da equipe técnica institucional.

2.9.4. Os equipamentos e softwares fornecidos deverão ser novos, sem uso anterior, em linha de fabricação do fabricante e compatíveis com o ambiente tecnológico atualmente utilizado no âmbito da Universidade do Estado do Rio de Janeiro - UERJ, observando os requisitos de padronização, interoperabilidade, integração e gerenciamento centralizado definidos institucionalmente.

2.9.5. A solução deverá possibilitar operação em alta disponibilidade, suporte às funcionalidades avançadas de segurança de rede, integração com mecanismos de autenticação, segmentação de tráfego, inspeção de aplicações, VPN, prevenção de intrusões, filtragem web, análise de ameaças e demais recursos compatíveis com soluções corporativas de segurança de perímetro.

2.9.6. Além disso, deverão ser observadas as exigências relacionadas à garantia, suporte técnico especializado, atualização contínua das bases de proteção e disponibilidade de atendimento pelo fabricante ou representante autorizado no território nacional, durante toda a vigência contratual.

2.10. Definição da natureza

2.10.1. Os itens que integram o objeto possuem características comuns e usuais encontradas no mercado de Tecnologia da Informação e Comunicação -TIC, cujos padrões de desempenho e qualidade podem ser objetivamente definidos, enquadrando-se, portanto, como bens e serviços comuns.

2.10.2. O objeto da contratação contempla solução de segurança de perímetro composta por appliances de firewall corporativo, solução de gerenciamento centralizado de logs e treinamento operacional, observados os seguintes aspectos:

a) Os itens de appliance firewall, transceivers ópticos e console de gerenciamento de logs são medidos em unidades e correspondem ao fornecimento de bens, incluindo hardware, licenciamento, garantia, instalação, configuração e suporte técnico;

b) O item de treinamento operacional é medido por aluno/vaga e corresponde à prestação de serviço especializado de capacitação técnica da equipe responsável pela administração da solução.

2.11. Condições gerais

2.11.1. Todos os equipamentos, licenças, subscrições, softwares, acessórios e demais componentes fornecidos deverão ser novos, sem uso anterior, em linha de fabricação do fabricante e destinados ao mercado corporativo, não sendo admitidos produtos recondicionados, remanufaturados, usados ou descontinuados.

2.11.2. A solução deverá ser entregue completa e em pleno funcionamento, contemplando todos os componentes necessários à sua instalação, integração, operação e gerenciamento, ainda que não expressamente mencionados neste Termo de Referência, sem ônus adicional para a CONTRATANTE.

2.11.3. Todos os equipamentos, licenças e subscrições deverão possuir cobertura de garantia e suporte técnico pelo prazo de 60 (sessenta) meses, observadas as condições estabelecidas neste Termo de Referência.

2.11.4. A CONTRATADA será responsável pela instalação, configuração, migração do ambiente existente, execução dos testes de funcionamento, documentação da solução implantada e transferência de conhecimento à equipe técnica do HUPE.

2.11.5. Os equipamentos e licenças deverão ser registrados em nome do Hospital Universitário Pedro Ernesto - HUPE, garantindo acesso aos portais do fabricante, atualizações de software, firmwares, assinaturas de segurança, documentação técnica e abertura de chamados de suporte.

2.11.6. A solução fornecida deverá ser compatível com a infraestrutura tecnológica existente no HUPE e observar os requisitos de padronização tecnológica adotados institucionalmente pela UERJ.

2.11.7. A CONTRATADA deverá assegurar que todos os componentes fornecidos operem de forma integrada, responsabilizando-se pela compatibilidade entre hardware, software, licenças, transceivers e demais elementos que compõem a solução.

2.11.8. Eventuais custos relacionados a transporte, frete, seguros, tributos, instalação, configuração, migração, testes, treinamento e demais despesas necessárias ao perfeito cumprimento do objeto deverão estar incluídos na proposta comercial da CONTRATADA .

2.11.9. A solução deverá atender integralmente às especificações técnicas, funcionais, operacionais e de segurança previstas neste Termo de Referência.

2.12. Condição de fornecimento do serviço

2.12.1. Para que a solução de segurança de perímetro atenda plenamente às necessidades do HUPE, faz-se necessária a contratação de fornecimentos e serviços acessórios indispensáveis à correta implantação, integração, operação e sustentação da solução principal.

2.12.2. Além dos appliances de firewall e da solução de gerenciamento centralizado de logs e eventos, deverão ser contemplados os respectivos licenciamentos, subscrições de segurança, suporte técnico especializado, garantia do fabricante, módulos de conectividade (transceivers) necessários à integração com a infraestrutura existente, bem como os serviços de instalação, configuração, migração do ambiente atual, realização de testes operacionais e treinamento da equipe técnica responsável pela administração da solução.

2.12.3. Tais fornecimentos são essenciais para assegurar que os equipamentos sejam entregues em pleno funcionamento, devidamente integrados ao ambiente computacional institucional e aptos a prover os níveis de segurança, disponibilidade e desempenho requeridos pelo HUPE.

2.12.4. A necessidade desses componentes acessórios foi identificada durante o levantamento de mercado e corroborada pela análise de contratações similares realizadas por órgãos e entidades públicas, nas quais se verificou que soluções de firewall corporativo são normalmente CONTRATADA s de forma integrada, contemplando não apenas os equipamentos, mas também os serviços técnicos e licenciamentos necessários à sua efetiva operacionalização.

2.12.5. Dessa forma, os fornecimentos acessórios não constituem objetos independentes, mas elementos indispensáveis à adequada execução da solução pretendida, contribuindo para a redução de riscos operacionais, garantia da continuidade dos serviços e maximização dos resultados esperados com a contratação.

3 - DESCRIÇÃO DA SOLUÇÃO:

A solução a ser CONTRATADA consiste no fornecimento de **solução integrada de segurança de perímetro de rede**, composta por **02 (dois) appliances FortiGate 200G**, configurados em **Alta Disponibilidade (High Availability - HA)**, **01 (uma) solução virtual FortiAnalyzer VM** para gerenciamento centralizado de logs e eventos de segurança, **06 (seis) transceptores ópticos SFP+ 10Gb SR**, licenciamento, subscrições de segurança, garantia e suporte técnico do fabricante pelo período de **60 (sessenta) meses**, bem como serviços especializados de instalação, configuração, migração do ambiente existente, testes de funcionamento, documentação técnica e treinamento operacional da equipe técnica do Hospital Universitário Pedro Ernesto - HUPE.

A solução deverá prover mecanismos avançados de segurança de rede (Next Generation Firewall - NGFW), contemplando funcionalidades de inspeção profunda de pacotes, sistema de prevenção contra intrusão (IPS), controle de aplicações, filtragem de conteúdo Web e DNS, inspeção SSL/TLS, proteção contra malwares, VPN IPsec e SSL, segmentação de redes, alta disponibilidade, roteamento dinâmico, gerenciamento centralizado e demais recursos necessários à proteção do ambiente computacional institucional.

A contratação abrange, de forma integrada, o fornecimento do hardware, licenciamento, subscrições de segurança, garantia do fabricante, suporte técnico especializado, serviços de implantação, configuração, migração assistida do ambiente atualmente em operação, execução dos testes de homologação, entrega da documentação técnica da solução implantada e capacitação da equipe técnica da CONTRATANTE, assegurando a plena operacionalização da infraestrutura de segurança durante toda a vigência contratual.

A solução deverá integrar-se à infraestrutura tecnológica atualmente utilizada pela Universidade do Estado do Rio de Janeiro - UERJ, observando os requisitos de padronização tecnológica institucional, compatibilidade com o ecossistema Fortinet existente, continuidade operacional, segurança da informação, proteção dos dados pessoais sensíveis tratados pelo HUPE e gerenciamento centralizado dos ativos de segurança de rede.

3.1. Duração do contrato

Uma vez que a contratação contempla solução de Tecnologia da Informação e Comunicação - TIC composta por fornecimento de equipamentos, licenciamento, suporte técnico, garantia e atualização de assinaturas de segurança por período determinado, o prazo de vigência do contrato será de **60 meses**, contados a partir da data da publicação no Portal Nacional de Contratações Públicas (PNCP), podendo ser prorrogado conforme Art. 107, da Lei 14.133/2021.

3.2. Reajuste de preços

O reajustamento de preços ocorrerá conforme o índice IPCA, após período de 12 meses, em caso de haver prorrogação contratual, conforme Art. 107, da Lei 14.133/2021.

3.3. Garantia

3.3.1. A cobertura de garantia contratual será avaliada de acordo com a OS-003-GDG-2024, conforme documento SEI-260007/003437/2024, obedecendo as cláusulas previstas no Art. 96 da Lei 14.133/21.

3.4. Critérios e práticas de sustentabilidade

3.4.1. A CONTRATADA deverá promover a correta destinação dos resíduos resultantes da prestação do serviço, tais peças substituídas, embalagens, entre outros, observando a legislação e princípios de responsabilidade socioambiental (Lei nº 12.305/2010).

3.4.2. Deverá ainda obedecer aos critérios previstos no capítulo I do Decreto 43.629/2012, por meio dos artigos 1º e 2º, in verbis:

Art. 1º - As especificações para a aquisição de bens, contratação de serviços e obras por parte dos órgãos e entidades da Administração Pública Estadual Direta e Indireta, a fixação de critérios de julgamento e a execução e fiscalização dos respectivos contratos, observarão critérios de sustentabilidade ambiental, na forma deste Decreto.

Art. 2º - Consideram-se critérios de sustentabilidade ambiental, dentre outros:

I - economia no consumo de água e energia;

II - minimização da geração de resíduos e destinação final ambientalmente adequada dos que forem gerados;

III - racionalização do uso de matérias-primas; IV - redução da emissão de poluentes;

V - adoção de tecnologias menos agressivas ao meio ambiente; VI - implementação de medidas que reduzam as emissões de gases de efeito estufa e aumentem os sumidouros;

VII - utilização de produtos de baixa toxicidade;

VIII- utilização de produtos com a origem ambiental sustentável comprovada, quando existir certificação para o produto.

3.5. Possibilidade de subcontratação

3.5.1. Não será permitida a subcontratação, cessão, transferência ou qualquer forma de sub-rogação, total ou parcial, do objeto da contratação, tendo em vista sua natureza indivisível e a necessidade de fornecimento integrado da solução, estruturada em lote único composto por itens de caráter permanente.

3.5.2. Ressalta-se que a eventual realização de treinamento diretamente pelo fabricante da solução, ou por meio de plataforma oficial a ele vinculada, não será caracterizada como subcontratação, cessão ou transferência, por se tratar de atividade inerente à própria solução fornecida e integrante do escopo contratado.

3.6. Possibilidade de participação de Consórcio

3.6.1. É vedada a participação de pessoas jurídicas reunidas em consórcio.

3.6.2. A vedação se dá em razão das características específicas da solução a ser CONTRATADA, que não pressupõe multiplicidade ou heterogeneidade de atividades empresariais distintas, nem envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital.

3.6.3. Entende-se que os itens a serem contratados não exigem empresas de diferentes segmentos e/ou capacidades reunidas para atuarem na execução do objeto proposto.

3.6.4. Ademais, a gestão compartilhada poderá gerar vícios ou lacunas no fluxo dos processos de atendimento. A cadeia de responsabilidades entre as empresas será maior que se o objeto estiver sob responsabilidade de uma única empresa, ainda que operacionalizado por meio de atuação conjunta com outras empresas.

3.6.5. Mesmo a garantia produzida como consequência da aquisição é resultado de equipes, técnicas e procedimento complementar, não havendo benefício ou necessidade de segmentação para a realização

do objeto proposto, além de repercutir em vários canais de atendimento de eventuais chamados técnicos, gerando uma morosidade no atendimento e ocasionando o não cumprimento dos itens expostos no edital.

3.6.6. A ausência de consórcio não trará prejuízos à competitividade do certame, visto que, em regra, a formação de consórcios é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital. Nestes casos, a Administração, com vistas a aumentar o número de participantes, admite a formação de consórcio.

3.6.7. Tendo em vista que é prerrogativa do Poder Público, na condição de CONTRATANTE, a escolha da participação ou não de empresas constituídas sob a forma de consórcio, com as devidas justificativas, conforme a literalidade do texto da Lei nº o 14.133, art 15 e seus incisos e parágrafos, pelos motivos já expostos, conclui-se que a vedação de constituição de empresas em consórcio, para o caso concreto, é o que melhor atende o interesse público, por prestigiar os princípios da competitividade, economicidade e moralidade.

3.6.8. Por fim, a vedação da participação de empresas reunidas em regime de consórcio visa exatamente afastar a restrição à competição, na medida em que a reunião de empresas que, individualmente, poderiam fornecer os equipamentos, reduziria o número de licitantes e poderia, eventualmente, proporcionar a formação de conluios/cartéis para manipular os preços nas licitações

3.7. Possibilidade de participação de Cooperativa

3.7.1. Não será admitida a participação de cooperativa de trabalho, qualquer que seja a sua forma de constituição, já que o objeto principal trata de compra de bens de aquisição perpétua e, no caso dos itens secundários de treinamento, há vínculo de subordinação direta entre o empregado e a empresa CONTRATADA para a prestação dos serviços.

3.8. Reserva de cota de Microempresa, Empresa de Pequeno Porte e Microempreendedor Individual

3.8.1. Após análise das características da contratação pretendida, concluiu-se pela impossibilidade de aplicação dos benefícios previstos nos artigos 47 e 48 da Lei Complementar nº 123/2006, referentes à participação exclusiva ou à reserva de cotas para Microempresas (ME) e Empresas de Pequeno Porte (EPP).

3.8.2. A contratação envolve solução corporativa de segurança da informação de elevada complexidade técnica, abrangendo o fornecimento de appliances especializados, licenciamento de software, subscrições de segurança, suporte técnico do fabricante, integração com o ambiente institucional existente e serviços especializados associados, demandando capacidade operacional, técnica e comercial compatível com os requisitos da solução.

3.8.3 Além disso, a necessidade de padronização tecnológica e compatibilidade com a infraestrutura corporativa atualmente utilizada no âmbito da Universidade do Estado do Rio de Janeiro - UERJ exige que os fornecedores possuam capacidade técnica e autorização do fabricante para fornecimento, implantação e suporte da solução adotada institucionalmente.

3.8.4. Adicionalmente, o valor estimado da contratação supera o limite previsto para realização de licitação exclusiva para Microempresas e Empresas de Pequeno Porte, não se mostrando tecnicamente viável o parcelamento da solução em cotas independentes, uma vez que a segregação dos componentes poderia comprometer a integração, a interoperabilidade, o gerenciamento unificado e a adequada execução da solução de segurança pretendida.

3.8.5. Dessa forma, conclui-se pela não aplicação de licitação exclusiva ou reserva de cotas para Microempresas e Empresas de Pequeno Porte na presente contratação.

3.8.6. Ressalta-se, contudo, que não haverá impedimento à participação de Microempresas e Empresas de Pequeno Porte no certame, desde que atendam integralmente às exigências de

habilitação jurídica, qualificação técnica, qualificação econômico-financeira e demais requisitos estabelecidos no instrumento convocatório.

3.9. Incidência do Programa de Integridade

3.9.1. Para a presente contratação, será exigida da empresa licitante vencedora a comprovação da existência de um Programa de Integridade (Compliance), que deverá ser apresentado antes da assinatura do contrato.
3.9.2. Justificativa e Fundamentação Legal:

3.9.3. A exigência fundamenta-se na Lei Estadual nº 7.753/2017, que estabelece a obrigatoriedade de implementação de Programa de Integridade para empresas que celebrem contratos com a Administração Pública direta, indireta e fundacional do Estado do Rio de Janeiro, cujos valores sejam superiores a R$ 650.000,00 (seiscentos e cinquenta mil reais), no caso de compras e serviços, e cujo prazo de vigência seja igual ou superior a 180 (cento e oitenta) dias.

3.9.4. Considerando que o valor estimado da presente contratação ultrapassa o limite estabelecido na referida legislação estadual, bem como que o prazo contratual previsto será superior a 180 (cento e oitenta) dias, a exigência de Programa de Integridade torna-se obrigatória para a futura CONTRATADA .

3.9.5. Ressalta-se que, embora a Lei nº 14.133/2021 preveja a obrigatoriedade de implementação de Programa de Integridade apenas para contratações de grande vulto (art. 25, §4º), a norma estadual possui aplicação específica no âmbito do Estado do Rio de Janeiro, devendo ser observada por esta Administração.

3.9.6. Adicionalmente, em consonância com a Lei nº 14.133/2021, destaca-se que a existência de Programa de Integridade apresenta reflexos relevantes no processo licitatório e na gestão contratual, tais como:

- Critério de desempate: poderá ser utilizado como critério de desempate entre propostas, nos termos do art. 60, inciso IV;
- Atenuante na aplicação de sanções: será considerada como circunstância atenuante na eventual aplicação de penalidades administrativas, conforme disposto no art. 156, §1º, inciso V

4 - REQUISITOS MÍNIMOS PARA EXECUÇÃO:

4.1. Qualificação Técnica

4.1.1. Para fins de comprovação da qualificação técnica, a licitante deverá apresentar um ou mais atestados de capacidade técnica, emitidos por pessoa jurídica de direito público ou privado, em nome da licitante, que comprovem aptidão para fornecimento, licenciamento, garantia, suporte técnico, instalação, implantação, configuração ou sustentação de solução de segurança de rede, firewall, UTM, NGFW, centralização/análise de logs ou solução tecnicamente equivalente, em características, quantidades e prazos compatíveis com o objeto da contratação.

4.1.2. Os atestados deverão comprovar atividade pertinente e compatível com o objeto, preferencialmente abrangendo fornecimento de appliances ou equipamentos de segurança de rede, licenciamento, suporte oficial de fabricante, instalação, implantação, configuração, migração, centralização de logs ou atividades correlatas.

4.1.3. Para fins de aferição da compatibilidade quantitativa, poderá ser exigida comprovação de execução anterior correspondente a até 50% do quantitativo ou dimensão do objeto a ser contratado, observada a proporcionalidade, a razoabilidade e a validação pela área competente responsável pela elaboração do edital.

4.1.4. Será admitido o somatório de atestados, desde que os objetos comprovados sejam tecnicamente compatíveis entre si e, em conjunto, demonstrem capacidade para execução do fornecimento, implantação, licenciamento, suporte técnico e garantia pretendidos.

4.1.5. Os atestados deverão conter informações suficientes para verificação de sua autenticidade e compatibilidade com o objeto, incluindo, sempre que possível, identificação da CONTRATANTE, descrição do objeto executado, quantitativos, prazos, local de execução e dados de contato do responsável pela emissão.

4.1.6. A Administração poderá realizar diligências para comprovar a legitimidade dos atestados apresentados, solicitando, quando necessário, contrato, nota fiscal, ordem de fornecimento, termo de recebimento, endereço atual da CONTRATANTE, local de execução ou outros documentos pertinentes.

4.1.7. A licitante deverá apresentar documento emitido pelo fabricante, distribuidor autorizado ou canal oficial, tal como declaração, carta de solidariedade, carta de autorização ou documento equivalente, comprovando que os itens ofertados serão fornecidos por canal regular e contarão com suporte e garantia oficiais no Brasil pelo prazo mínimo de 60 (sessenta) meses.

4.1.8. A licitante deverá apresentar catálogos, datasheets, declarações ou documentação técnica oficial que comprove os modelos, part numbers, características técnicas, compatibilidades, licenças, subscrições e níveis de suporte ofertados.

4.1.9. A comprovação de registro ou ativação da solução no portal oficial do fabricante poderá ser exigida como condição para o recebimento definitivo do objeto, sem prejuízo da apresentação prévia dos documentos de habilitação e proposta.

4.1.10. A exigência de certificações técnicas específicas de profissionais somente será admitida quando proporcional, tecnicamente justificada e validada pela área competente, de modo a evitar restrição indevida à competitividade do certame.

5 - MODELO DE GESTÃO E FISCALIZAÇÃO DO CONTRATO:

5.1. Instrumentos necessários

5.1.1. Para a adequada execução, acompanhamento e fiscalização do contrato, serão utilizados, no mínimo, os seguintes instrumentos:

5.1.1.1. Termo de ciência de designação, contendo a manifestação expressa dos agentes designados para atuação como gestor e fiscal do contrato, nos termos do art. 10 do Decreto nº 48.817/2023;

5.1.1.2. Ato de designação dos agentes responsáveis pela gestão e fiscalização do contrato, publicado no Diário Oficial do Estado;

5.1.1.3. Termo de Referência;

5.1.1.4. Mapa de Riscos;

5.1.1.5. Documentos de habilitação da CONTRATADA ;

5.1.1.6. Registro de ocorrências, destinado ao acompanhamento da execução contratual, no qual serão anotados os eventos relevantes, falhas, comunicações e demais informações pertinentes;

5.1.1.7. Instrumento contratual firmado entre as partes, ou documento equivalente;

5.1.1.8. Demais documentos e registros necessários ao acompanhamento da execução do contrato.

5.2. Agentes que participarão da gestão do contrato

5.2.1. Em conformidade com o disposto no Decreto nº 48.817/2023, que regulamenta a gestão e a fiscalização das contratações no âmbito do Estado do Rio de Janeiro, a execução contratual será acompanhada por agentes formalmente designados pela Administração, conforme as atribuições descritas a seguir:

5.2.1.1. **Gestor do contrato**: servidor designado pela autoridade competente, responsável pela coordenação geral da execução contratual, devendo possuir capacidade técnica e conhecimento compatível com o objeto da contratação;

5.2.1.2. **Fiscalização do contrato**: será exercida por servidor(es) designado(s), em quantidade e com perfil compatível com a complexidade do objeto, podendo compreender:

5.2.1.2.1. **Fiscal técnico:** responsável pelo acompanhamento dos aspectos técnicos da execução do objeto, devendo possuir conhecimentos compatíveis com a solução de tecnologia da informação CONTRATADA , nos termos do art. 5º, inciso I, do Decreto nº 48.817/2023;

5.2.1.2.2. **Fiscal administrativo:** responsável pelo acompanhamento dos aspectos administrativos da execução contratual, incluindo a conferência de documentação, apoio ao processo de pagamento e verificação do cumprimento das obrigações formais da CONTRATADA ;

5.2.1.3. Na hipótese de não haver designação específica de fiscal administrativo, suas atribuições poderão ser absorvidas pelo(s) fiscal(is) técnico(s), conforme definido pela Administração.

5.3. Rotinas de Fiscalização

5.3.1. Cabe à Fiscalização Técnica:

- Acompanhar a execução dos serviços quanto aos aspectos técnicos, verificando a conformidade da solução com as especificações estabelecidas neste Termo de Referência;
- Verificar a correta instalação, configuração e funcionamento da solução de segurança de endpoints;
- Monitorar a disponibilidade e o desempenho da solução, incluindo atualizações de segurança e funcionamento das licenças;
- Avaliar a qualidade do suporte técnico prestado pela CONTRATADA ;
- Registrar ocorrências, falhas ou irregularidades identificadas durante a execução contratual;
- Subsidiar o gestor do contrato com informações técnicas para tomada de decisão;
- Atestar a execução dos serviços para fins de recebimento e pagamento, quando verificada a conformidade.

5.3.2. Cabe à Fiscalização Administrativa:

- Conferir a documentação apresentada pela CONTRATADA para fins de pagamento;
- Verificar a regularidade fiscal e trabalhista durante a execução contratual, quando exigido;
- Apoiar o gestor do contrato no controle de prazos e vigência contratual;
- Auxiliar na instrução processual relacionada à execução do contrato.

5.3.3. Compete ao Gestor do Contrato:

- Coordenar a execução contratual, atuando como principal interlocutor junto à CONTRATADA ;
- Supervisionar as atividades de fiscalização técnica, administrativa e, quando houver, setorial;
- Avaliar a necessidade de aplicação de sanções administrativas, quando verificado descumprimento contratual;
- Controlar prazos contratuais, incluindo vigência e eventuais prorrogações;
- Autorizar, quando aplicável, a emissão de ordens de serviço ou instrumentos equivalentes;
- Consolidar informações para fins de prestação de contas e encerramento contratual;
- Encaminhar à autoridade competente demandas que extrapolem sua competência.

5.4. Obrigações das partes

5.4.1. Obrigações do CONTRATANTE

5.4.1.1. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA , de acordo com este Termo de Referência, contrato, edital, proposta e anexos.

5.4.1.2. Designar gestor e fiscais para acompanhamento, fiscalização, recebimento, validação técnica e ateste da execução contratual.

5.4.1.3. Fornecer à CONTRATADA as informações estritamente necessárias à execução do objeto, resguardadas informações sigilosas, sensíveis ou protegidas por norma interna.

5.4.1.4. Promover reunião de alinhamento com a CONTRATADA para definição dos procedimentos de entrega, instalação, implantação, migração, validação, comunicação e controle de mudanças.

5.4.1.5. Disponibilizar acesso físico e lógico controlado às dependências, sistemas e ambientes necessários à execução, desde que previamente autorizado, justificado e acompanhado.

5.4.1.6. Indicar janelas de mudança compatíveis com a criticidade do ambiente hospitalar e aprovar previamente atividades que possam afetar serviços, conectividade ou segurança.

5.4.1.7. Validar o Plano de Implantação, Plano de Reversão, cronograma e procedimentos técnicos apresentados pela CONTRATADA , quando aplicável.

5.4.1.8. Acompanhar a instalação, ativação, configuração, migração e testes, por meio da equipe técnica do HUPE/DESIT ou profissionais designados.

5.4.1.9. Conferir equipamentos, licenças, transceivers, part numbers, números de série, registros de suporte, documentação técnica, relatórios e demais evidências de conformidade.

5.4.1.10. Notificar a CONTRATADA , por escrito, sobre vícios, defeitos, incorreções, divergências de modelo, falhas de licenciamento, ausência de suporte ativo, atrasos ou qualquer desconformidade.

5.4.1.11. Recusar, total ou parcialmente, bens, licenças ou atividades que estejam em desacordo com as especificações, sem prejuízo das sanções cabíveis.

5.4.1.12. Realizar o recebimento provisório e definitivo nos termos deste Termo de Referência e da legislação aplicável.

5.4.1.13. Efetuar o pagamento devido à CONTRATADA após o recebimento definitivo, regular ateste e comprovação das condições contratuais, fiscais, orçamentárias e financeiras.

5.4.1.14. Fornecer, quando necessário, normas internas de segurança da informação, privacidade, confidencialidade, acesso físico, acesso lógico e controle de mudanças.

5.4.1.15. Adotar as providências internas cabíveis para a tramitação do processo conforme os fluxos institucionais e a governança estadual de TIC aplicável.

5.4.1.16. Aplicar sanções administrativas, glosas, retenções ou medidas cabíveis em caso de descumprimento contratual, observados o contraditório e a ampla defesa.

5.4.1.17. Dar ciência à área jurídica competente quando houver descumprimento relevante, necessidade de providência formal, apuração de responsabilidade ou dúvida jurídica.

5.4.2. Obrigações da CONTRATADA

5.4.2.1. Cumprir integralmente as condições deste Termo de Referência, contrato, edital, proposta e anexos.

5.4.2.2. Fornecer todos os equipamentos, licenças, subscrições, transceivers, suportes, garantias e atividades técnicas inerentes em conformidade com os modelos, part numbers, quantidades e requisitos técnicos exigidos.

5.4.2.3. Entregar equipamentos novos, originais, de primeiro uso, não recondicionados, não remanufaturados, não usados, livres de vícios, restrições, bloqueios, ônus ou impedimentos de registro e suporte.

5.4.2.4. Comprovar a origem regular dos bens, licenças e subscrições, bem como o fornecimento por canal autorizado do fabricante no Brasil, quando solicitado pela Administração.

5.4.2.5. Apresentar catálogo técnico, datasheet, declaração, certificado ou documento equivalente que comprove a aderência dos itens às especificações e aos part numbers indicados.

5.4.2.6. Ativar, registrar e comprovar o suporte oficial do fabricante pelo período de 60 meses, sem prejuízo de prazo superior ofertado em proposta.

5.4.2.7. Assegurar que os equipamentos, licenças e suportes estejam aptos à abertura de chamados, atualização, consulta de entitlement e exercício regular da garantia pelo HUPE.

5.4.2.8. Elaborar e submeter à aprovação da fiscalização técnica o Plano de Implantação, Plano de Reversão, cronograma, matriz de comunicação, procedimentos de teste e demais documentos necessários ao cumprimento dos níveis de serviço operacionais aplicáveis à implantação e migração.

5.4.2.9. Instalar, implantar, configurar e migrar os ativos atuais para os novos equipamentos, observadas as autorizações, janelas de mudança e controles definidos pelo HUPE/DESIT.

5.4.2.10. Realizar testes de funcionamento, conectividade, envio de logs, alta disponibilidade, ativação de licenças, suporte e demais verificações previstas no Plano de Implantação e na matriz de níveis de serviço operacionais aplicável à implantação e migração.

5.4.2.11. Entregar documentação técnica completa, relatório final de implantação, relatório de conformidade, evidências de testes, números de série, comprovantes de suporte, certificados/licenças e demais documentos exigidos.

5.4.2.12. Realizar repasse de conhecimento e orientação operacional à equipe técnica da CONTRATANTE, conforme escopo contratado.

5.4.2.13. Comunicar ao fiscal do contrato, por escrito e tão logo constatado, qualquer fato que possa impactar a entrega, ativação, suporte, garantia, implantação, migração ou execução do objeto.

5.4.2.14. Substituir, corrigir, reparar ou complementar, às suas expensas, item entregue em desconformidade, com defeito, divergência técnica, falha de licenciamento, irregularidade de suporte ou documentação insuficiente.

5.4.2.15. Manter sigilo absoluto sobre informações, dados, topologias, endereços, regras, credenciais, logs, relatórios, vulnerabilidades, incidentes, documentos e especificações técnicas a que tiver acesso.

5.4.2.16. Observar a LGPD, a legislação de segurança da informação, as normas internas da CONTRATANTE e os termos de confidencialidade aplicáveis.

5.4.2.17. Não divulgar, reproduzir, compartilhar, publicar ou utilizar informações da CONTRATANTE para finalidade diversa da execução contratual.

5.4.2.18 Comunicar à CONTRATANTE, em até 24 horas, qualquer incidente ou suspeita de incidente de segurança da informação, acesso indevido, perda, vazamento, alteração, comunicação ou tratamento inadequado de dados, logs, credenciais ou documentos sob sua responsabilidade.

5.4.2.19. Indicar preposto ou responsável técnico para interlocução com a CONTRATANTE, quando solicitado.

5.4.2.20. Participar de reuniões de alinhamento, acompanhamento, validação técnica e encerramento, sempre que convocada.

5.4.2.21. Manter durante toda a vigência contratual as condições de habilitação e qualificação exigidas na licitação.

5.4.2.22. Responsabilizar-se por todos os custos diretos e indiretos relacionados ao fornecimento, incluindo tributos, frete, seguro, descarregamento, licenciamento, ativação, suporte, garantia, deslocamentos e demais encargos.

5.4.2.23. Responsabilizar-se por danos causados à Administração ou a terceiros em decorrência de ação ou omissão sua, de seus empregados, prepostos ou subcontratados autorizados.

5.4.2.24. Abster-se de contratar, para atuação no objeto, agente público ou pessoa vedada pela legislação, observadas as regras de conflito de interesses.

5.4.2.25. Não desativar, alterar ou intervir em recursos computacionais da CONTRATANTE sem autorização formal da fiscalização técnica.

5.4.2.26. Apresentar, quando solicitado, evidências de abertura de chamados junto ao fabricante, histórico de suporte, status de RMA, atualização de licenças e demais informações necessárias à

fiscalização.

5.4.2.27. Não permitir utilização de trabalho de menor de dezesseis anos, exceto na condição de aprendiz a partir de quatorze anos, nem de menor de dezoito anos em trabalho noturno, perigoso ou insalubre, nos termos constitucionais e legais aplicáveis.

5.4.2.28. Arcar com o ônus decorrente de eventual equívoco no dimensionamento de sua proposta, devendo complementar, às suas expensas, tudo o que for necessário ao atendimento integral do objeto, quando o previsto inicialmente não for suficiente para cumprir as especificações exigidas.

5.5. Indicadores de desempenho e qualidade da solução

5.5.1. Durante o período de garantia e suporte técnico, a fiscalização acompanhará o desempenho da solução por meio de indicadores objetivos destinados a verificar a disponibilidade dos equipamentos, a efetividade do suporte técnico, a manutenção das licenças e subscrições, a atualização dos mecanismos de segurança e o adequado funcionamento dos componentes fornecidos.

5.5.2. Os indicadores previstos neste item possuem finalidade exclusivamente gerencial e de fiscalização da execução contratual, não constituindo mecanismo de remuneração variável nem Acordo de Nível de Serviço típico de contratos continuados.

5.5.3. Indicadores mínimos de desempenho

5.5.3.1 Serão adotados, no mínimo, os seguintes indicadores:

a) Disponibilidade da solução

Os appliances de firewall e a solução de gerenciamento de logs deverão permanecer operacionais durante toda a vigência contratual, ressalvadas as interrupções previamente autorizadas para manutenção programada.

b) Atendimento aos chamados técnicos

Todos os chamados registrados pela CONTRATANTE deverão observar os prazos máximos de atendimento e solução definidos neste Termo de Referência, conforme sua classificação de criticidade.

c) Atualizações da solução

A CONTRATADA deverá assegurar a disponibilidade contínua das atualizações de firmware, assinaturas de segurança, mecanismos de proteção e demais subscrições CONTRATADA s junto ao fabricante durante todo o período de vigência contratual.

d) Garantia e suporte do fabricante

A solução deverá permanecer registrada junto ao fabricante durante toda a vigência do contrato, garantindo acesso aos serviços oficiais de suporte técnico, RMA, atualizações e base de conhecimento.

e) Disponibilidade do gerenciamento centralizado

A solução FortiAnalyzer deverá permanecer operacional, garantindo a recepção, armazenamento, consulta e geração de relatórios dos eventos de segurança produzidos pelos appliances de firewall.

5.5.4. Forma de aferição

5.5.4.1. A verificação dos níveis de serviço será realizada mediante:

a) relatórios emitidos pelos próprios equipamentos FortiGate e FortiAnalyzer;

b) registros do portal oficial do fabricante;

c) registros de chamados técnicos;

d) relatórios apresentados pela CONTRATADA ;

e) registros produzidos pela fiscalização contratual;

f) testes de funcionamento realizados pela CONTRATANTE, quando aplicáveis.

5.5.5. Registro de ocorrências

5.6.5.1. Todas as falhas, indisponibilidades, interrupções, degradações de desempenho ou descumprimentos dos níveis de serviço deverão ser registradas pela fiscalização do contrato.

5.6.5.2. As ocorrências serão classificadas conforme seu impacto operacional:

a) Baixo impacto: falhas que não comprometam a operação da solução ou possuam alternativa operacional temporária.

b) Médio impacto: falhas que afetem parcialmente funcionalidades da solução, sem interrupção completa dos serviços.

c) Alto impacto: falhas que provoquem indisponibilidade total da solução, perda de redundância, comprometimento da segurança da informação ou indisponibilidade de serviços críticos do HUPE.

5.5.6. Consequências do descumprimento

5.6.6.1.O descumprimento reiterado dos indicadores poderá ensejar registro de ocorrência, determinação de adoção de medidas corretivas, aplicação das penalidades previstas contratualmente, retenção do recebimento definitivo quando cabível e demais medidas previstas na legislação:

a) registro da ocorrência pela fiscalização;

b) notificação formal da CONTRATADA ;

c) determinação de adoção de medidas corretivas;

d) aplicação das sanções previstas na Lei nº 14.133/2021 e neste Termo de Referência;

5.6. Recebimento provisório e definitivo do objeto

5.6.1. O recebimento provisório ocorrerá após a entrega física e documental dos bens, para fins de conferência inicial de quantidade, integridade, modelo, part number, número de série, documentação fiscal, documentação técnica, licenças e demais evidências iniciais de conformidade.

5.6.2. O recebimento definitivo somente ocorrerá após a validação técnica da conformidade dos itens, ativação das licenças, comprovação do suporte oficial por 60 meses, registro no fabricante, verificação da documentação exigida, saneamento de pendências e, quando aplicável, testes de funcionamento, implantação, migração e integração.

5.6.3. O recebimento definitivo não afasta a responsabilidade da CONTRATADA por vícios, defeitos, inconsistências, incompatibilidades, irregularidades de licenciamento, falhas de suporte, violações de sigilo ou desconformidades identificadas posteriormente.

5.6.4. Serão recusados os itens entregues em desconformidade com as especificações, com part number divergente, sem suporte oficial ativo, sem comprovação de origem regular, usados, recondicionados, remanufaturados, com garantia inferior à exigida, incompatíveis com a solução pretendida ou sem documentação técnica suficiente.

5.6.5. O aceite definitivo deverá considerar, além da entrega dos bens e licenças, a conclusão satisfatória das atividades técnicas inerentes ao fornecimento, a entrega de relatório final, a realização dos testes pactuados, a documentação das configurações e o repasse de conhecimento à equipe do HUPE/DESIT.

5.6.6. A fiscalização poderá emitir termo de recebimento com ressalvas quando houver pendências que não comprometam a operação da solução, fixando prazo para saneamento, sem prejuízo da retenção, glosa ou aplicação de sanções quando cabível.

5.6.7. A presente contratação não se caracteriza como contrato continuado de prestação de serviços com dedicação exclusiva de mão de obra, razão pela qual não se aplica Acordo de Nível de Serviço (ANS) para fins de medição mensal da execução contratual. Contudo, considerando que a implantação ocorrerá em ambiente hospitalar crítico, serão observados indicadores operacionais de implantação destinados exclusivamente ao acompanhamento dos marcos de entrega, qualidade técnica, gestão da mudança, testes, documentação e estabilização da solução, conforme matriz constante deste item.

5.6.8. Os níveis de serviço operacionais previstos neste item não descaracterizam a natureza da contratação como aquisição de solução de TIC, nem transformam as atividades de instalação, implantação, migração, ativação, configuração assistida, testes, documentação e repasse de conhecimento em serviço continuado ou item autônomo de contratação.

5.6.9 O ANS operacional incidirá exclusivamente sobre as etapas críticas de transição, implantação e estabilização inicial, devendo ser aferido pela fiscalização técnica com base nos registros do processo, relatórios da CONTRATADA , evidências de testes, atas de reunião, plano de implantação, plano de reversão e demais documentos exigidos neste Termo de Referência.

5.6.10 A execução das atividades sujeitas ao ANS deverá observar as janelas de mudança aprovadas pelo HUPE/DESIT, a criticidade dos serviços hospitalares, a necessidade de preservação da continuidade operacional e a vedação de intervenção em ambiente produtivo sem autorização formal ou registro equivalente da fiscalização técnica.

5.6.11. Para fins de acompanhamento, deverão ser observados, no mínimo, os seguintes indicadores operacionais, sem prejuízo de detalhamento ou ajuste pelo edital, contrato, Ordem de Fornecimento, Plano de Implantação ou decisão motivada da fiscalização:

Indicador operacional	Prazo/parâmetro	Evidência mínima	Consequência do descumprimento
Reunião de alinhamento inicial	Até 5 dias úteis após assinatura/publicação ou Ordem de Fornecimento, salvo ajuste da Administração.	Ata, e-mail ou registro equivalente com responsáveis, cronograma, riscos e próximos passos.	Registro de ocorrência, reprogramação motivada e sanções se o atraso for imputável à CONTRATADA .
Plano de Implantação e Plano de Reversão	Até 5 dias úteis após a reunião de alinhamento ou prazo validado pelo HUPE/DESIT.	Plano com escopo, cronograma, dependências, janelas, testes, riscos e reversão.	Não autorização de intervenção produtiva, devolução para correção, retenção de aceite e sanções cabíveis.
Janela de mudança	Agendamento com antecedência mínima de 2 dias úteis, salvo autorização excepcional.	Solicitação formal, aprovação da fiscalização e comunicação aos envolvidos.	Intervenção não autorizada poderá caracterizar descumprimento contratual e risco à segurança operacional.
Comunicação de riscos, impedimentos ou incidentes	Imediata para eventos críticos e até 4 horas úteis para eventos não críticos identificados pela CONTRATADA .	Comunicação ao fiscal/gestor com evento, impacto, causa provável e providências.	Registro de falha de comunicação, plano corretivo e responsabilização por agravamento do risco.

Testes técnicos mínimos	Antes do pedido de recebimento provisório e após cada intervenção relevante.	Relatório de testes de conectividade, HA, logs, licenças, suporte, atualização e funcionamento básico.	Não recebimento provisório ou definitivo até o saneamento das pendências.
Acionamento do Plano de Reversão	Imediato após decisão da fiscalização ou identificação de falha crítica que comprometa a continuidade operacional.	Registro da decisão, horários, responsáveis, procedimentos executados e resultado da reversão.	Registro de ocorrência grave, apuração de responsabilidade e aplicação das medidas contratuais cabíveis.
Saneamento de inconformidade impeditiva de aceite	Prazo definido pela fiscalização, preferencialmente até 2 dias úteis para pendências documentais ou de configuração não complexas.	Relatório de correção, evidência técnica, documento complementar ou comprovação de substituição.	Retenção do aceite, glosa quando cabível, recusa do item/atividade e sanções previstas.
Relatório final e repasse de conhecimento	Relatório final em até 3 dias úteis após a implantação/migração; repasse em até 5 dias úteis ou data acordada.	Relatório final, documentação as built, evidências, lista de presença, roteiro ou material de apoio.	Pendência impeditiva de recebimento definitivo, salvo dispensa formal da Administração.
Estabilização inicial	Estabilização inicial em até 7 dias úteis após implantação/migração.	Registros de acompanhamento, chamados, validação de logs e ajustes necessários ao aceite definitivo.	Exigência de saneamento, retenção do aceite e demais providências previstas no contrato.

5.6.12. Os prazos previstos na matriz acima poderão ser ajustados pela Administração no edital, contrato, Ordem de Fornecimento ou Plano de Implantação aprovado, conforme criticidade, complexidade, janela de mudança, disponibilidade de equipe, dependências do ambiente e necessidade de preservação da continuidade hospitalar.

5.6.13. O descumprimento dos níveis de serviço operacionais não implicará medição mensal típica de contrato continuado, mas poderá ensejar registro de ocorrência, exigência de plano corretivo, retenção do recebimento, glosa da parcela afetada quando cabível, recusa de item ou atividade, aplicação de sanções administrativas e demais providências previstas no edital, contrato e legislação aplicável.

5.6.14. Não será imputado à CONTRATADA o descumprimento de indicador quando comprovado que o atraso ou impedimento decorreu exclusivamente de fato atribuível à Administração, indisponibilidade de janela de mudança, dependência técnica não informada previamente, força maior, caso fortuito ou outro evento devidamente justificado e aceito pela fiscalização.

5.6.15. Durante a fase de estabilização inicial, pelo período de 7 dias úteis após a implantação/migração, a CONTRATADA deverá apoiar a fiscalização técnica na verificação de funcionamento, saneamento de pendências, validação de logs, abertura ou escalonamento de chamados junto ao fabricante e ajustes necessários à consolidação do aceite definitivo, nos limites do escopo contratado.

5.6.17. O pedido de recebimento provisório deverá ser instruído pela CONTRATADA com a documentação técnica completa, incluindo, conforme aplicável, relatório de testes, inventário com

números de série e part numbers, comprovantes de licenciamento, evidências de registro e suporte no fabricante, documentação as built, arquivos de configuração autorizados, relatório de implantação, pendências e evidências de integração.

5.6.16. O recebimento provisório ocorrerá após a entrega dos equipamentos, licenças, documentação inicial e demais componentes do objeto, bem como após a conclusão das atividades cuja execução anteceda a implantação em ambiente produtivo, mediante termo circunstanciado ou registro equivalente, para conferência física, documental e técnica inicial.

5.6.18. A fiscalização técnica deverá verificar a aderência dos bens e atividades às especificações, a integridade dos equipamentos, a compatibilidade dos part numbers, a ativação das licenças, o registro do suporte, o funcionamento básico da solução, a entrega documental e o saneamento das pendências registradas.

5.6.19. A fiscalização administrativa, quando designada, deverá verificar os documentos fiscais, a regularidade documental, a conformidade da nota fiscal, a manutenção das condições de habilitação e demais requisitos necessários à liquidação e ao pagamento.

5.6.20. Havendo irregularidades que impeçam a liquidação ou o recebimento definitivo, a fiscalização deverá registrar as inconformidades, indicar as exigências não atendidas e solicitar à CONTRATADA a correção, substituição, complementação ou saneamento no prazo fixado.

5.6.21. O recebimento definitivo ocorrerá após a verificação da qualidade, quantidade, conformidade técnica, regularidade documental, ativação de suporte/licenças, conclusão das atividades inerentes ao fornecimento e saneamento das pendências impeditivas.

5.6.22. Na hipótese de controvérsia quanto à execução, qualidade, quantidade ou conformidade, poderá ser reconhecida apenas a parcela incontroversa, conforme avaliação da fiscalização e orientação da área competente, sem prejuízo da apuração das responsabilidades cabíveis.

5.6.23. Nenhum prazo de recebimento ou pagamento correrá enquanto houver pendências imputáveis à CONTRATADA que impeçam a conferência, a liquidação, a emissão de aceite ou a validação técnica do objeto.

5.6.24. O recebimento provisório ou definitivo não exclui a responsabilidade civil, técnica, administrativa ou contratual da CONTRATADA por vícios, defeitos, falhas de licenciamento, suporte irregular, desconformidade posterior, danos ou imperfeições constatadas após o aceite.

5.6.25. A própria CONTRATADA não poderá substituir a avaliação de desempenho, qualidade ou conformidade de responsabilidade da fiscalização, sem prejuízo da apresentação de relatórios, evidências e documentos técnicos que subsidiem a análise da Administração.

5.6.26. O recebimento definitivo deverá ser acompanhado de termo, parecer, despacho ou registro equivalente, com indicação dos itens recebidos, documentos avaliados, ressalvas, pendências saneadas e responsáveis pela validação.

5.7. Pagamento

5.7.1. O pagamento será realizado em **três parcelas**, mediante a apresentação de nota fiscal (ou documento equivalente), após o recebimento definitivo do objeto, conforme as condições estabelecidas neste Termo de Referência.

5.7.2. O pagamento ficará condicionado à comprovação, pela CONTRATADA , da entrega do objeto, ativação da solução, conclusão dos serviços de instalação e configuração, bem como da plena operacionalização da solução no ambiente da CONTRATANTE.

5.7.3. A CONTRATADA deverá emitir documentos fiscais distintos para cada unidade administrativa, observando os respectivos dados de faturamento e os quantitativos de licenças a elas destinados, conforme definido neste Termo de Referência.

5.7.4. As notas fiscais deverão ser emitidas em nome da **Universidade do Estado do Rio de Janeiro - UERJ**, CNPJ nº **33.540.014/0001-57**, Inscrição Estadual nº **76.003.939**, devendo conter a descrição detalhada dos serviços prestados e dos itens fornecidos, em conformidade com o objeto contratado.

5.7.5. Toda a comunicação relacionada à execução contratual poderá ser realizada por meio do endereço eletrônico: **desit.contratos@hupe.uerj.br**, sem prejuízo de outros meios formais definidos pela CONTRATANTE.

5.7.6. Considera-se ocorrido o recebimento da nota fiscal no momento em que a fiscalização do contrato atestar a execução do objeto, em conformidade com as condições estabelecidas.

5.7.7. A nota fiscal deverá ser apresentada após a emissão do respectivo **Termo de Recebimento Definitivo**, conforme previsto neste Termo de Referência.

5.7.8. Caso seja constatada divergência entre a nota fiscal apresentada e os serviços efetivamente prestados, a fiscalização notificará a CONTRATADA para proceder à correção ou substituição do documento, no prazo de até **10 (dez) dias corridos**, ficando suspenso o prazo para pagamento até a regularização.

6 - REMUNERAÇÃO DO OBJETO:

6.1. A remuneração da CONTRATADA será realizada pelo fornecimento integral da solução de segurança de perímetro de rede, compreendendo os appliances FortiGate 200G, a solução virtual FortiAnalyzer VM, transceptores ópticos, licenciamento, subscrições de segurança, garantia e suporte oficial do fabricante pelo período de 60 (sessenta) meses, bem como os serviços de instalação, configuração, migração, testes, documentação técnica e treinamento operacional, conforme especificações constantes deste Termo de Referência.

6.2. O valor contratado deverá contemplar todos os custos necessários à perfeita execução do objeto, incluindo equipamentos, software, licenças, subscrições, garantia, suporte técnico do fabricante, instalação, configuração, migração, testes, documentação técnica, treinamento, transporte, seguros, tributos, encargos trabalhistas, previdenciários, fiscais, comerciais e quaisquer outras despesas diretas ou indiretas indispensáveis ao cumprimento das obrigações contratuais.

6.3. A proposta comercial deverá ser apresentada considerando o **valor global do lote**, correspondente ao fornecimento integral da solução, não sendo admitida cobrança adicional por componentes, serviços, licenças, acessórios, atualizações, deslocamentos ou quaisquer outros itens necessários ao perfeito funcionamento da solução CONTRATADA .

6.4. A remuneração compreenderá todos os itens e serviços descritos neste Termo de Referência, incluindo aqueles que, embora não expressamente discriminados na proposta comercial, sejam indispensáveis à completa instalação, integração, funcionamento, homologação e operação da solução, sem ônus adicional para a CONTRATANTE.

6.5. O pagamento será realizado após o recebimento definitivo do objeto, observadas as condições estabelecidas neste Termo de Referência, no contrato e na legislação aplicável, mediante apresentação da documentação exigida e atesto da fiscalização competente.

7 - JULGAMENTO DAS PROPOSTAS:

7.1. A presente contratação será realizada por meio da modalidade **pregão, em sua forma eletrônica**, tendo como critério de julgamento das propostas o **menor preço**, considerando o **valor global do lote**, nos termos do Decreto nº 48.778/2023 e da Lei nº 14.133/2021.

7.2. As propostas deverão ter validade mínima de **60 (sessenta) dias**, contados da data de sua apresentação, salvo disposição diversa no edital.

7.3. As propostas deverão contemplar todos os custos necessários à execução do objeto, incluindo, hardware, fornecimento de licenças, serviços de instalação, configuração, suporte técnico, tributos, encargos e demais despesas diretas e indiretas.

7.4. Não será exigida apresentação de amostras, prova de conceito ou testes de conformidade, tendo em vista que a solução possui características padronizadas de mercado, conforme demonstrado no Estudo Técnico Preliminar.

7.5. Em caso de empate entre propostas, serão aplicados os critérios de desempate previstos no art. 60 da Lei nº 14.133/2021.

8 - SANÇÕES ADMINISTRATIVAS:

8.1. No caso de descumprimento total ou parcial das condições deste Termo de Referência e do correspondente instrumento de contratação, o Hospital Universitário Pedro Ernesto, sem prejuízo das perdas e danos e das multas cabíveis, nos termos da lei civil, aplicará à **CONTRATADA** , conforme o caso, as penalidades previstas nos artigos 155 a 163 da Lei Federal nº 14.133/21, bem como, no que couber, as disposições contidas na Lei Estadual nº 287/79 e suas regulamentações.

8.2. Constituem hipóteses de infração, entre outras: atraso injustificado, entrega de item incompatível, fornecimento sem suporte oficial, ausência de comprovação de licença, descumprimento de prazo ou de nível de serviço operacional aplicável, falha de garantia, violação de sigilo, tratamento inadequado de dados, recusa de substituição, implantação inadequada, migração não autorizada e inexecução total ou parcial.

8.3. As sanções poderão incluir advertência, multa, impedimento de licitar e contratar e declaração de inidoneidade, observados o contraditório, a ampla defesa e os critérios de dosimetria previstos na legislação e no instrumento convocatório.

8.4. A aplicação de sanção não afasta a obrigação de reparar danos, substituir itens, regularizar licenças, corrigir documentação, concluir implantação ou cumprir demais obrigações contratuais pendentes.

8.5. A aplicação de sanções deverá observar registro formal das ocorrências, indicação das obrigações descumpridas, comunicação à CONTRATADA , contraditório, ampla defesa, dosimetria e encaminhamento à autoridade competente, nos termos da legislação e dos normativos internos aplicáveis.

9 - DISPOSIÇÕES GERAIS:

9.1. O início da execução dos serviços deverá ser formalmente autorizado pela CONTRATANTE, por meio de instrumento próprio, tais como ordem de serviço, autorização formal ou documento equivalente, emitido pela área competente.

9.2. A licitante deverá, antes da apresentação da proposta, realizar todos os levantamentos necessários ao adequado dimensionamento dos serviços, não sendo admitidas, posteriormente, alegações de desconhecimento das condições para execução do objeto como justificativa para descumprimento contratual ou solicitação de reequilíbrio econômico-financeiro.

9.3. A apresentação da proposta implica plena aceitação das condições estabelecidas neste Termo de Referência e no edital, bem como o compromisso de executar o objeto nos seus exatos termos.

9.4. O valor proposto deverá contemplar todos os custos necessários à execução do objeto, incluindo licenças, serviços de instalação, configuração, suporte técnico, capacitação, tributos, encargos sociais, trabalhistas, previdenciários, logísticos e quaisquer outras despesas diretas ou indiretas.

10 - RESPONSÁVEIS PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA:

Responsável: Dimitri dos Santos

Matrícula: 36.656-7

ID Funcional: 4441625

Telefone: (21) 2868-8686

E-mail institucional: dimitri.santos@hupe.uerj.br

Responsável: Pedro Augusto Ferreira Figueiredo Lopes

Matrícula: 37.047-8

ID Funcional: 4458438

Telefone: (21) 2868-8686 | Ramal: 1002

E-mail institucional: pedro.lopes@hupe.uerj.br

Rio de Janeiro, 15 setembro de 2026

Documento assinado eletronicamente por **Dimitri dos Santos**, **Técnico de Informática**, em 15/09/2026, às 18:08, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022 .

Documento assinado eletronicamente por **Pedro Augusto F. de Figueiredo Lopes**, **Técnico de Informática**, em 15/09/2026, às 18:08, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **141592704** e o código CRC **F769DF2D**.

Referência: Processo nº SEI-260007/003004/2026 SEI nº 141592704