Estudo Técnico Preliminar 94/2025

1. Informações Básicas

Número do processo: 25029.000474/2025-21

2. Descrição da necessidade

2.1. O Instituto Nacional de Infectologia Evandro Chagas (INI), um dos Institutos da Fundação Oswaldo Cruz, contribui significativamente para a atenção de referência, para a vigilância e para o desenvolvimento de ações voltadas ao enfrentamento das doenças infecciosas no Brasil, particularmente, no Estado do Rio de Janeiro. A peculiaridade de seu perfil assistencial também faz do INI o principal Centro de Referência de Pesquisa Clínica, Vigilância e Ensino em doenças infecciosas dentre todas as Unidades da Fiocruz.

O INI entende como sua Missão “Produzir conhecimento e tecnologias para melhorar a saúde da população, por meio de ações integradas de pesquisa, atenção à saúde, ensino e vigilância, com interface humana-animal-ambiente, tendo como Valores centrais o compromisso com o SUS e a redução das iniquidades”. Como Visão de futuro o INI se propõe a “Ser reconhecido como liderança nacional e internacional em pesquisa e atenção à saúde em Doenças Infecciosas, com alta capacidade de articulação e resposta rápida para o enfrentamento das ameaças à Saúde Pública”.

Em 2010, por meio da publicação da Portaria nº 4.160 do MS, passou a ser definido como Instituto Nacional de Infectologia Evandro Chagas, para atuar como órgão auxiliar do MS na formulação de políticas públicas, no planejamento, no desenvolvimento, na coordenação e na avaliação das ações integradas para a saúde na área da infectologia.

No campo da pesquisa e ensino, o INI se caracteriza pela excelência na pesquisa clínica, na assistência de elevado padrão de qualidade, no ensino para formar e capacitar novos profissionais na área e parcerias estabelecidas com instituições nacionais e internacionais nessas áreas de atividade.

No campo da Vigilância em Saúde, cinco Laboratórios/Serviço de Referência do INI atuam no diagnóstico de doenças, desenvolvendo atividades no aperfeiçoamento de metodologias e capacitação de profissionais nas seguintes áreas: Tuberculose e Micobacterioses não Tuberculosas; Micoses Sistêmicas; Leishmaniose Tegumentar Americana e Referência Regional para Leishmaniose Visceral; Diagnóstico microscópico da malária para a Região Extra-Amazônica e Diagnóstico Histológico de Doenças Infecciosas. Com essa estrutura, o INI apoia o MS na vigilância epidemiológica, prevenção e controle de agravos, exercendo papel estratégico para o SUS.

O INI possui também uma estrutura assistencial de Hospital-Dia voltada para o atendimento às diversas situações que dispensam internação hospitalar. Para além da estrutura hospitalar, conta com um ambulatório referenciado, realizando imunizações especiais e atendimento para medicina do viajante, micoses profundas como histoplasmose, criptococose, esporotricose e outras dermatozoonoses, assim como atendimento multiprofissional para portadores HIV/AIDS e outras ISTs, Mpox, neuroinfecções, síndromes respiratórias causadas por influenza, coronavírus, paracoccidioidomicose pulmonar, tuberculose e síndromes febris agudas. A Unidade tem protagonismo na prevenção ao HIV/AIDS, buscando alcançar impacto na redução de novas infecções.

Assim, considerada a necessidade estratégica e a possibilidade de pesquisar-se sobre uma doença, a Unidade deve prover infraestrutura adequada para o atendimento aos respectivos

usuários, garantindo que os recursos humanos e tecnológicos estejam alinhados com as melhores práticas e inovações na área da saúde, promovendo um ambiente seguro e eficiente para a pesquisa e tratamento. Dessa forma, a Unidade poderá oferecer um suporte integral e de qualidade, atendendo às necessidades específicas de cada usuário e contribuindo para o avanço científico e a melhoria contínua dos serviços prestados.

O INI mostrou sua relevância com papel ativo nas grandes emergências sanitárias nacionais como foi o caso da Doença de Chagas, da AIDS e das doenças febris agudas. Mais recentemente, exerceu grande protagonismo no enfrentamento da pandemia de Covid-19 e demonstrou capacidade de rápida mobilização quando, fruto de uma parceria entre o MS e a Fiocruz, permitiu a assistência de milhares de cidadãos acometidos pelo coronavírus, com a construção do Centro Hospitalar com capacidade para até 195 leitos, atualmente com 120 leitos operacionais. A requalificação do Centro Hospitalar durante o ano de 2022 permitiu o avanço em sua missão de fortalecer o SUS por meio de atenção de referência, pesquisas de ponta, geração de protocolos assistenciais e formação de profissionais nos diferentes níveis formativos.

A obsolescência do firewall atual expõe a instituição a riscos críticos de segurança cibernética, tornando-a vulnerável a ataques cada vez mais sofisticados. A aquisição imediata de um NGFW é imprescindível para proteger as informações confidenciais dos pacientes e garantir a integridade das pesquisas.

A expansão do Instituto Nacional de Infectologia com o novo centro hospitalar, aliada ao aumento exponencial de dispositivos conectados à rede, torna a aquisição de um Firewall de Próxima Geração (NGFW) uma necessidade urgente. O NGFW protegerá a rede do INI, garantindo a confidencialidade das informações dos pacientes, especialmente os dados sensíveis. Com suas funcionalidades avançadas de inspeção de pacotes e prevenção contra ameaças, o NGFW oferecerá uma proteção robusta contra ataques cibernéticos, assegurando a continuidade dos serviços e a integridade dos dados institucionais.

3. Área requisitante

Área Requisitante	Responsável
Serviço de Tecnologia da Informação e Comunicação – SETIC	THIAGO LOURENCO CAVALCANTE

4. Necessidades de Negócio

4.1. Garantir a segurança e integridade das informações confidenciais de pacientes e dados de pesquisa, frente à crescente sofisticação das ameaças cibernéticas e à obsolescência do firewall atual.

4.2. Assegurar a continuidade dos serviços assistenciais e de pesquisa, minimizando interrupções causadas por incidentes de segurança.
4.3. Proteger a infraestrutura de rede do INI, que se expandiu com o novo centro hospitalar e o aumento significativo de dispositivos conectados.

4.4. Manter a conformidade com as legislações vigentes relacionadas à proteção de dados e segurança da informação, como a Lei Geral de Proteção de Dados (LGPD).

4.5. Fortalecer a reputação do INI como instituição de excelência em saúde, garantindo a confiança dos usuários e parceiros na segurança de seus dados.

5. Necessidades Tecnológicas

5.1. Substituir o firewall obsoleto por uma solução moderna e eficaz de Firewall de Próxima

Geração (NGFW).

5.2. Implementar funcionalidades avançadas de segurança, incluindo inspeção profunda de pacotes, controle de aplicações, filtragem de conteúdo web, sistema de prevenção de intrusões (IPS) e antivírus/antimalware embarcado.

5.3. Garantir alta disponibilidade (HA) para assegurar a resiliência da rede e minimizar o tempo de inatividade em caso de falhas.

5.4. Prover suporte a múltiplos contextos virtuais (VDOMs ou equivalentes) para segregação lógica de redes e otimização de recursos.

5.5. Permitir integração com sistemas existentes, como Active Directory, LDAP e SIEM, para otimização da gestão de segurança e autenticação de usuários.

5.6. Oferecer capacidade de SD-WAN nativa para balanceamento inteligente de múltiplos links e otimização do tráfego de rede.

5.7. Assegurar suporte técnico especializado e garantia de longo prazo (mínimo de 60 meses) para a manutenção e atualização contínua da solução.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

6.1. A solução deve apresentar as certificações e conformidades mínimas listadas na descrição complementar dos itens (Common Criteria EAL 4+, ICSA Labs Firewall Certification, FIPS 140-2, ISO/IEC 15408, CE e FCC Class A), garantindo a aderência a padrões internacionais de segurança.

6.2. O fornecedor deverá comprovar autorização como revenda oficial do fabricante da solução ofertada, garantindo a procedência e o suporte direto.

6.3. O fornecedor deverá apresentar atestado de capacidade técnica que comprove fornecimento prévio de solução NGFW equivalente (mínimo 50% do volume licitado), atestando sua experiência e capacidade de execução.

6.4. A equipe técnica do fornecedor deverá possuir profissionais certificados conforme exigido na descrição complementar dos itens (ITIL Foundation v3 ou superior, PMP (PMI), CISSP e certificação na tecnologia ofertada), garantindo a qualificação para implementação e suporte.

6.5.
6.6. A solução deve prever atendimento on-site obrigatório, com SLA de atendimento para substituição de hardware de no máximo 4 horas úteis, assegurando a rápida recuperação em caso de falhas críticas.

6.7. A solução deve incluir atualizações de firmware e assinaturas durante todo o período de garantia, garantindo proteção contínua contra novas ameaças.

7. Estimativa da demanda - quantidade de bens e serviços

ITEM	CATMAT	DESCRIÇÃO CATMAT	DESCRIÇÃO COMPLEMENTAR	UND	QTE

1	609340	FIREWALL, APLICAÇÃO: SEGURANÇA REDE COMPUTADORES, MODELO: APLIANCE NGFW	Aparelho NGFW TIPO 1: Throughput NGFW 8 Gbps. VPN IPSEC 40 Gbps. IPS 10 Gbps. SSL Inspection 6 Gbps. Suporte a 6.500.000 conexões simultâneas. Suporte a 400.000 conexões novas por segundo. 16 portas 1GbE RJ45. 6 portas 10GbE SFP+. Suporte nativo ou licenciado a 8 contextos virtuais (VDOMs ou equivalentes). Controle de aplicações com reconhecimento por assinatura e comportamento. Filtro de conteúdo web (URL Filtering). Sistema de prevenção contra intrusões (IPS). Antivírus e antimalware embarcado. SSL Inspection (inbound/outbound). Suporte a NAT, DHCP, VLAN, LACP, VRRP, BGP, OSPF, RIPv2, SNMP, sFlow. Integração com Active Directory e LDAP para identificação e autenticação de usuários. Suporte a SD-WAN nativa, com balanceamento de múltiplos links. Criação de políticas por aplicação, usuário, localização geográfica, horário e risco. Suporte a criação de VPNs IPSEC e SSL. Gerenciamento via Web (HTTPS) e CLI (SSH). Suporte a logs via Syslog, SNMP e integração com SIEM. Suporte a modos de operação Sniffer, L2, L3. Suporte a alta disponibilidade (HA) em modo ativo-passivo e ativo-ativo. CERTIFICAÇÕES E CONFORMIDADES MÍNIMAS: Common Criteria EAL 4+. ICSA Labs Firewall Certification. FIPS 140-2. ISO/IEC 15408. CE e FCC Class A. GARANTIA E SUPORTE: Garantia mínima de 60 meses (5 anos) fornecida diretamente pelo fabricante. Atendimento on-site obrigatório, com possibilidade de suporte remoto para incidentes de menor criticidade. SLA de atendimento com tempo máximo de substituição de hardware de 4 horas úteis. Suporte técnico 24x7 (telefone, e-mail e portal), com resposta inicial em até 1h. Atualizações de firmware e assinaturas inclusas durante todo o período. CONDIÇÕES DE ENTREGA: Equipamentos novos, lacrados de fábrica. Fornecimento de todos os acessórios necessários (fontes, cabos, manuais). EXIGÊNCIAS DO FORNECEDOR: Comprovação de autorização como revenda oficial do fabricante. Atestado de capacidade técnica que comprove fornecimento prévio de solução NGFW equivalente (mínimo 50% do volume licitado). Profissionais certificados exigidos: 1 x ITIL Foundation v3 ou superior, 1 x PMP (PMI). 1 x CISSP. 1 x certificado na tecnologia ofertada.	UN	2

2	609340	FIREWALL, APLICAÇÃO: SEGURANÇA REDE COMPUTADORES, MODELO: APLIANCE NGFW	Aparelho NGFW TIPO 2: Throughput NGFW 600 Mbps. VPN IPSEC 5 Gbps. IPS 1 Gbps. SSL Inspection 500 Mbps. Suporte a 500.000 conexões simultâneas. Suporte a 30.000 conexões novas por segundo. 8 portas 1GbE RJ45. Suporte nativo ou licenciado a 2 contextos virtuais. Controle de aplicações com reconhecimento por assinatura e comportamento. Filtro de conteúdo web (URL Filtering). Sistema de prevenção contra intrusões (IPS). Antivírus e antimalware embarcado. SSL Inspection (inbound/outbound). Suporte a NAT, DHCP, VLAN, LACP, VRRP, BGP, OSPF, RIPv2, SNMP, sFlow. Integração com Active Directory e LDAP para identificação e autenticação de usuários. Suporte a SD-WAN nativa, com balanceamento de múltiplos links. Criação de políticas por aplicação, usuário, localização geográfica, horário e risco. Suporte a criação de VPNs IPSEC e SSL. Gerenciamento via Web (HTTPS) e CLI (SSH). Suporte a logs via Syslog, SNMP e integração com SIEM. Suporte a modos de operação Sniffer, L2, L3. Suporte a alta disponibilidade (HA) em modo ativo-passivo e ativo-ativo. CERTIFICAÇÕES E CONFORMIDADES MÍNIMAS: Common Criteria EAL 4+. ICSA Labs Firewall Certification. FIPS 140-2. ISO/IEC 15408. CE e FCC Class A. GARANTIA E SUPORTE: Garantia mínima de 60 meses (5 anos) fornecida diretamente pelo fabricante. Atendimento on-site obrigatório, com possibilidade de suporte remoto para incidentes de menor criticidade. SLA de atendimento com tempo máximo de substituição de hardware de 4 horas úteis. Suporte técnico 24x7 (telefone, e-mail e portal), com resposta inicial em até 1h. Atualizações de firmware e assinaturas inclusas durante todo o período. CONDIÇÕES DE ENTREGA: Equipamentos novos, lacrados de fábrica. Fornecimento de todos os acessórios necessários (fontes, cabos, manuais). EXIGÊNCIAS DO FORNECEDOR: Comprovação de autorização como revenda oficial do fabricante. Atestado de capacidade técnica que comprove fornecimento prévio de solução NGFW equivalente (mínimo 50% do volume licitado). Profissionais certificados exigidos: 1 x ITIL Foundation v3 ou superior, 1 x PMP (PMI). 1 x CISSP. 1 x certificado na tecnologia ofertada.	UN	2

7.1. Definição do método para a estimativa das quantidades:

7.1.1. A quantidade estimada para esta aquisição, compreendendo duas unidades de NGFW Tipo 1 e duas unidades de NGFW Tipo 2, foi dimensionada para atender integralmente às necessidades operacionais e estratégicas do INI – Instituto Nacional de Infectologia Evandro Chagas. Essa estimativa baseou-se em uma análise criteriosa da infraestrutura de rede existente, da demanda crescente por segurança cibernética decorrente da expansão do Instituto (incluindo o novo centro hospitalar) e do volume de dados sensíveis a serem protegidos.

A alocação de equipamentos de diferentes capacidades (Tipo 1 para o core da rede e Tipo 2 para pontos específicos com menor tráfego, por exemplo) otimiza o investimento, garantindo a proteção adequada em cada segmento, sem sub ou superdimensionar os recursos.

Além disso, a previsão de redundância (HA) para os equipamentos essenciais foi um fator determinante para as quantidades, assegurando a continuidade dos serviços e a alta disponibilidade da infraestrutura de segurança. A solução proposta visa prover uma cobertura robusta e escalável para as atividades atuais e futuras do INI, alinhando-se às melhores práticas de segurança da informação para ambientes de missão crítica.

8. Levantamento de soluções

8.1. Foram levantadas diversas soluções de Firewall de Próxima Geração (NGFW) disponíveis no mercado, considerando as funcionalidades e requisitos técnicos específicos para atender às necessidades do INI. As soluções foram pesquisadas junto a fabricantes renomados e seus revendedores autorizados, buscando identificar aquelas que melhor se adequam ao perfil de segurança e infraestrutura da instituição.

9. Análise comparativa de soluções

9.1. Não se aplica. (Considerando que a descrição complementar já detalha os requisitos técnicos mínimos, a análise comparativa de soluções seria parte de um processo posterior de pesquisa de mercado para identificação de fornecedores, conforme a IN 65/2021).

10. Registro de soluções consideradas inviáveis

10.1. Não se aplica. (Da mesma forma que o item anterior, a inviabilidade de soluções seria identificada em um estágio mais avançado da pesquisa de mercado, após a análise detalhada das propostas).

11. Análise comparativa de custos (TCO)

11.1. Não se aplica. (A análise de TCO – Total Cost of Ownership – seria realizada após a coleta de propostas de preços e detalhamento dos custos de manutenção, licenças e suporte de cada solução, o que ocorrerá na fase de pesquisa de preços da licitação).

A razão pela qual "não se aplica” colocados nos itens 9.1 e 11.1 é dado ter o documento ETP o objetivo de demonstrar a viabilidade técnica e econômica da solução escolhida.

Este estudo já apresenta uma descrição detalhada da necessidade e dos requisitos tecnológicos e de negócio, além de já descrever a solução de TIC a ser contratada, com especificações técnicas bem definidas (NGFW Tipo 1 e Tipo 2).

A análise comparativa de soluções e de custos (TCO), conforme a lógica apresentada no ETP e alinhada à IN 65/2021, é uma etapa que se aprofunda e é formalizada na fase de pesquisa de preços. Aqui, já foi definido a necessidade de um NGFW com determinadas características. A comparação detalhada das diversas opções de mercado (marcas, modelos) e a análise do Custo Total de Propriedade (TCO) de cada uma delas, com base em propostas e outros dados de mercado, serão realizadas no momento oportuno pelo setor responsável, durante a fase de pesquisa de preços para a licitação, como mencionado no item 13.1.

Portanto, neste ponto, a análise é mais estratégica sobre a necessidade e a escolha do tipo de solução (NGFW) e não sobre a comparação detalhada entre diferentes produtos ou fornecedores, o que será feito na pesquisa de preços, seguindo os preceitos da IN 65/2021.

12. Descrição da solução de TIC a ser contratada

12.1. A solução de TIC a ser contratada consiste na aquisição de 4 (quatro) unidades de Firewall de Próxima Geração (NGFW), sendo 2 (duas) unidades do Tipo 1 e 2 (duas) unidades do Tipo 2, conforme as especificações detalhadas no item 7. A escolha por dois tipos distintos de equipamentos visa atender às necessidades de diferentes pontos da rede do INI, otimizando o custo-benefício e garantindo a capacidade de processamento e segurança adequada para cada ambiente. A solução deverá integrar funcionalidades avançadas de segurança, alta disponibilidade e capacidade de gerenciamento centralizado, proporcionando uma proteção abrangente e eficaz contra ameaças cibernéticas. Além disso, a contratação engloba a garantia mínima de 60 meses (5 anos) diretamente do fabricante, incluindo atendimento on-site, suporte técnico especializado 24x7 e atualizações de firmware e assinaturas durante todo o período, assegurando a longevidade e o desempenho contínuo dos equipamentos.

13. Estimativa de custo total da contratação

14. Justificativa técnica da escolha da solução

14.1. A escolha por uma solução de Firewall de Próxima Geração (NGFW) é tecnicamente justificada pela necessidade premente de aprimorar a segurança da rede do INI, que atualmente se encontra vulnerável devido à obsolescência do firewall existente. Um NGFW oferece uma abordagem de segurança mais robusta e proativa, indo além das capacidades dos firewalls tradicionais. As funcionalidades exigidas, como inspeção profunda de pacotes (DPI), controle de aplicações, filtragem de conteúdo web, sistema de prevenção de intrusões (IPS) e antivírus/antimalware embarcado, são essenciais para identificar e mitigar ameaças sofisticadas, como ataques de dia zero, malwares avançados e tentativas de exfiltração de dados. A capacidade de suporte a múltiplos contextos virtuais permitirá a segregação lógica de redes para diferentes departamentos ou projetos, garantindo maior granularidade no controle de acesso e na aplicação de políticas de segurança. A inclusão de SD-WAN nativa otimizará o uso dos links de internet, priorizando aplicações críticas e garantindo a continuidade dos serviços. Além disso, a exigência de alta disponibilidade (HA) em modo ativo-passivo ou ativo-ativo é crucial para assegurar que a proteção da rede não seja comprometida em caso de falha de um dos equipamentos. As certificações e conformidades solicitadas demonstram a aderência da solução a padrões internacionais de segurança da informação, conferindo maior confiabilidade e robustez. A garantia estendida e o suporte técnico on-site e remoto, com SLA rígido, garantem a sustentabilidade e a manutenção da solução ao longo do tempo, minimizando riscos operacionais.

15. Justificativa econômica da escolha da solução

15.1. A presente solicitação está em conformidade com o planejamento e orçamento aprovado

da Unidade. Existe disponibilidade orçamentária e financeira para a cobertura da despesa, conforme previsto no art. 40 da Lei nº 14.133/2021, inc. V, letra c.

ELEMENTO DE DESPESA: 44.90.52

UASG: 254492

PTRES: 172780

AÇÃO: 8305

15.2. O objeto da contratação está previsto no Plano de Contratações Anual 2025, conforme detalhamento a seguir:

Nº do DFD	Nº do Item no DFD	ID PCA no PNCP	Data de publicação no PNCP	ID DO ITEM NO PCA	Código Classe /Grupo	Código material /serviço	Identificador da Futura Contratação
209 /2024	1	33781055000135-0-000006/2025	27/03/2024	2085	6550	609340	254492-149/2025
	2			2087	6550	609340	

16. Benefícios a serem alcançados com a contratação

16.1. A aquisição do Firewall de Próxima Geração (NGFW) trará os seguintes benefícios para o INI:

- Aumento significativo da segurança cibernética: Proteção avançada contra ameaças como ransomware, phishing, ataques de dia zero e outras vulnerabilidades, salvaguardando dados sensíveis de pacientes e pesquisas.
- Conformidade regulatória: Atendimento aos requisitos da Lei Geral de Proteção de Dados (LGPD) e outras normas de segurança da informação, minimizando riscos legais e de reputação.
- Continuidade dos serviços: Redução drástica de interrupções nas operações devido a incidentes de segurança, garantindo a disponibilidade de sistemas críticos para a assistência à saúde e pesquisa.
- Otimização do desempenho da rede: Com funcionalidades como SD-WAN e controle de aplicações, a solução permitirá um uso mais eficiente da largura de banda e melhor experiência para os usuários.
- Gerenciamento simplificado e centralizado: A capacidade de gerenciamento via web e CLI, aliada à integração com SIEM, facilitará a administração da segurança e a resposta a incidentes.
- Redução de custos a longo prazo: Embora represente um investimento inicial, a prevenção de ataques e a redução de tempo de inatividade podem gerar economia significativa ao evitar perdas de dados, multas e custos de recuperação.
- Melhora da reputação institucional: Demonstrar um compromisso com a segurança da informação fortalece a imagem do INI junto a pacientes, colaboradores, parceiros e órgãos reguladores.

17. Providências a serem Adotadas

17.1. No específico desta contratação, não há necessidade de adequações/providências a

serem adotadas.

18. Descrição dos Requisitos da contratação

18.1. A presente contratação deve observar as seguintes lei e norma: Lei n° 14.133 de 1º de abril de 2021, que estabelece normas gerais de licitação e contratação para a Administração Pública e fundacionais da União, dos estados, do Distrito Federal e dos Municípios.

18.2 O fornecedor será selecionado por meio da realização de procedimento de Pregão Eletrônico.

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

Com base no estudo exposto acima, a Equipe de Planejamento, considera que a contratação do serviço em epígrafe é viável, além de ser necessária para o atendimento dos interesses da Administração.

20. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Despacho: INTEGRANTE REQUISITANTE

DIOGO VICENTE BITTENCOURT SACRAMENTO DIAS

Agente de contratação

Assinou eletronicamente em 11/07/2025 às 15:56:09.

Despacho: INTEGRANTE TÉCNICO

PATRICIA COSTA DOS SANTOS

Agente de contratação

Assinou eletronicamente em 09/07/2025 às 22:21:16.

Despacho: AUTORIDADE COMPETENTE DE TIC

THIAGO LOURENCO CAVALCANTE

Autoridade competente

Assinou eletronicamente em 14/07/2025 às 13:26:38.

Despacho: AUTORIDADE COMPETENTE

SOLANGE SIQUEIRA DUARTE DOS SANTOS

Autoridade competente

Assinou eletronicamente em 14/07/2025 às 14:42:33.