

Estudo Técnico Preliminar 223/2025

1. Informações Básicas

Número do processo: 60550.002645/2025-49

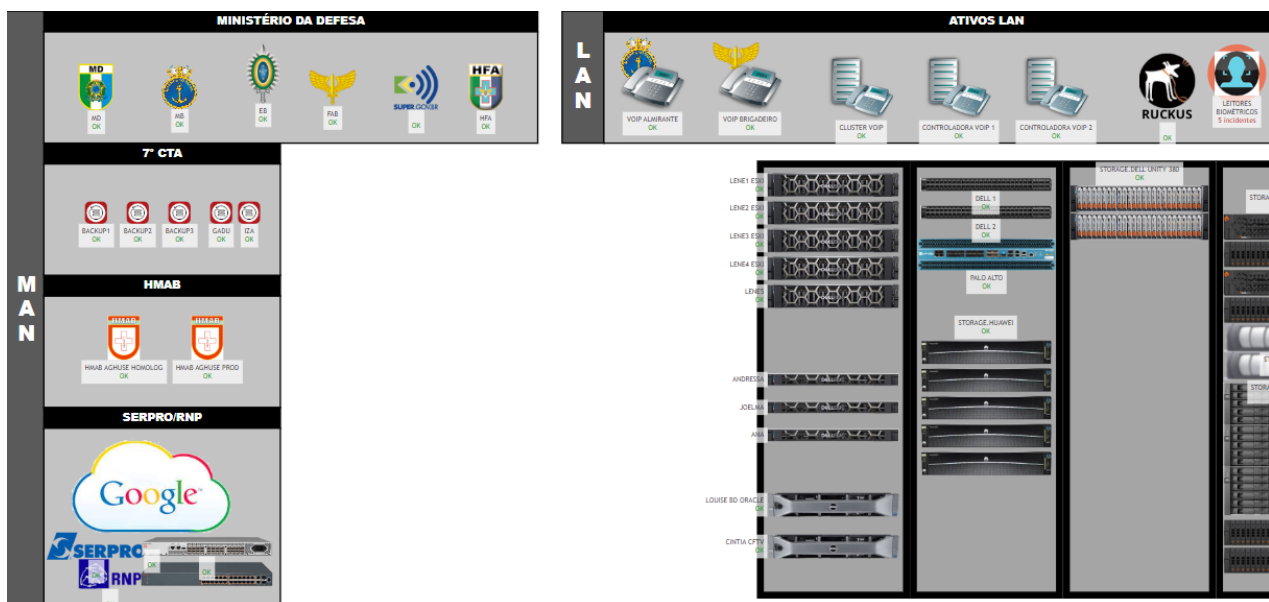
2. Descrição da necessidade

2.1. A Divisão de Tecnologia da Informação (DTI) tem como uma de suas atribuições, a de disponibilizar e gerir os recursos de Tecnologia da Informação e Comunicação (TIC) que sustentam as atividades do negócio do HFA. Para tanto, faz-se necessário analisar as necessidades de soluções de TIC, com vistas ao desenvolvimento ou à contratação de tais soluções.

2.2. *Compete a Seção de Segurança Cibernética assessorar a DTI, a planejar, implantar, administrar e manter os ativos de segurança de Tecnologia da Informação (TI) no âmbito do Hospital das Forças Armadas.*

2.3. A contratação alinha-se com o planejamento da Direção do HFA, de acordo com amparo ao Alinhamento com a Estratégia de Governança Digital para o período 2023 a 2026, no objetivo Estratégico OE3 *Melhorar a Infraestrutura Equipamentos e Instalações*. Em complemento, foi realizada uma consulta ao (PDTIC) 2023-2026 do HFA, cuja a necessidade M5 - Manter e adequar solução de Firewall dentro das melhores práticas e [A5.2 Aquisição de redundância do Firewall Palo Alto para atuação em alta disponibilidade .

2.4 Atualmente, a DTI mantém em funcionamento diversas ferramentas, e soluções de segurança de TI, que englobam equipamentos (hardwares) e sistemas (softwares), e que, trabalhando em conjunto, garantem níveis de segurança aceitáveis aos usuários da rede administrativa do HFA, no desenvolvimento de suas atividades laborais. Algumas dessas atividades estão demonstradas na figura abaixo:



2.5. As ferramentas e os equipamentos de segurança, responsáveis atualmente pelas proteções aos usuários da rede administrativa do HFA, estão suportados por contratos em fase de vigência e, portanto, os mesmos necessitam de manutenção, para que permitam garantir a segurança de TI da rede administrativa do HFA, em conformidade com os normativos vigentes, em especial à Lei Geral de Proteção de Dados Pessoais (LGPD Lei nº 13.709/2018).

2.6. Esta solicitação também está de acordo com a ORIENTAÇÃO NORMATIVA Nº 13 CMT LOG-HFA, DE 12 DE JANEIRO DE 2024, que dispõe sobre a Política de Segurança da Informação do Hospital das Forças Armadas (POSIN/HFA), no nº 4. DAS DIRETRIZES GERAIS, item 4.5 Gestão de incidentes de segurança da informação :

2.7. Os custodiantes da informação realizarão a gestão de incidentes envolvendo a segurança física e do ambiente.

2.8. De forma a promover a gestão e fomentar os aspectos de segurança da informação, a DTI – Divisão de Tecnologia da Informação, no âmbito da rede corporativa do HFA, deve: a) Instituir uma estrutura para a gestão de segurança da informação e comunicações.

2.9. Motivação/Justificativa

2.9.1. Atualmente o HFA possui em produção no ambiente de rede e proteção de dados, uma plataforma de NGFW, composta por Hardware e Softwares, da fabricante Palo Alto Networks, modelo **PA-3420**. Este equipamento está atuando como proteção de borda no ambiente do HFA. O objetivo deste processo é ampliar a proteção oferecida pelos firewalls de próxima geração (NGFW), por meio da substituição do equipamento de firewall modelo **PA-5220** atualmente em operação, por dois novos equipamentos modelo **PA-1410**, em arquitetura de alta disponibilidade, garantindo maior resiliência, desempenho e aderência aos padrões atuais de segurança cibernética, **visto que**, a solução hoje adotada do (**PA-5220**), não mais atende adequadamente as necessidades do nosocômio, já que apresenta limitações operacionais que comprometem sua capacidade de atender à demanda atual do ambiente do HFA. Como foi dito, a substituição será feita por dois equipamentos modelo PA-1410, tecnologia mais recente da fabricante Palo Alto Networks, que, além de apresentar novas funcionalidades em seu licenciamento, tem inclusão de Inteligência Artificial e “Machine Learning”. A escolha pelo modelo PA-1410 também se justifica por sua total compatibilidade com a plataforma de gerenciamento centralizado PANORAMA, já implementada no HFA, permitindo a administração unificada de políticas de segurança, atualizações, monitoramento e geração de relatórios. Esta integração proporciona eficiência operacional, padronização da gestão e maior visibilidade da segurança da rede como um todo, evitando a fragmentação da administração entre múltiplas interfaces ou fornecedores.

2.9.2 Além disso, a adoção de arquitetura em alta disponibilidade (H.A.) garante continuidade dos serviços mesmo em caso de falha de um dos dispositivos, elemento essencial no ambiente do HFA, altamente crítico, que demanda alta confiabilidade na operação dos sistemas de informação.

2.9.3. A demanda está alinhada aos objetivos estratégicos previstos no PDTIC HFA.

2.9.4. O objeto da contratação está previsto no Plano de Contratações Anual 2023-2026, conforme detalhamento a seguir:

2.9.4.1 ID PCA no PNCP: 03277610000125-0-000006/2025

2.9.4.2 Data de publicação no PNCP: 15/05/2024

2.9.4.3 Id do item no PCA: 630

2.9.4.4 Classe/Grupo: 7050 - EQUIPAMENTOS DE REDE DE TIC - LOCAL E REMOTA

2.9.4.7 Identificador da Futura Contratação: 112408-202/2025

2.9.5 Foi utilizada a ferramenta de busca de itens catalogados disponível no Portal de Compras do Governo Federal, <https://catalogo.compras.gov.br/cnbs-web/busca> e, conforme, anexo (**7752104**).

3. Necessidades de Negócio

4.1. Nesse sentido, para a continuidade e modernização das soluções de segurança existentes, são relacionadas as seguintes necessidades de negócio a serem atendidas:

4.1.1. Permitir que o HFA mantenha níveis adequados de segurança da informação, no que tange as ameaças provenientes de ataques externos e internos;

4.1.2. Manter a disponibilidade do ambiente de segurança da informação de forma ativa;

4.1.3. A proteção das estações de trabalho;

4.1.4. A proteção e o controle da Internet disponibilizada aos usuários;

4.1.5. Reduzir incidências de infecção causadas por malwares e de indisponibilidades do serviço de acesso internet;

4.1.6. A proteção dos sistemas corporativos;

4.1.7. A possibilidade de realizar varreduras de vulnerabilidades; e

4.1.8. A possibilidade de realizar auditorias e verificações de conformidade.

4.2. Garantir e evoluir a infraestrutura de TIC;

4.3. Proporcionar proteção a dados e informações trafegados nas redes do HFA , garantindo verificação, possibilidade de liberação ou bloqueio de tráfego de dados; e

4.3.1. Aumentar confiabilidade dos dados disponibilizados ao públicos.

4. Área requisitante

Área Requisitante	Responsável
Chefe da Subdivisão de Gestão de Tecnologia da Informação	Marco Antônio de Souza Farias - TC (EB)

5. Necessidades Tecnológicas

5.1. Garantir uma solução de firewall de próxima geração.

5.2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, otimizando a administração.

5.3. Garantir a proteção de acessos norte x sul (tráfego vertical – acesso internet) e leste x oeste (tráfego interno lateral) de forma integrada e otimizada.

5.4. A Divisão de Tecnologia da Informação já possui infraestrutura da rede de dados adequada de forma a permitir a instalação das licenças contratadas, com infraestrutura de rede elétrica adequada para energizar os ativos, sem a necessidade de desligamento de nenhum outro ativo em produção.

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

6.1. Melhorar substancialmente o nível de segurança da informação do hospital.

6.2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente

6.3. A prestadora dos serviços será responsável por disponibilizar todas as condições para a transferência de conhecimento, cabendo ao HFA demandar o repasse.

6.4. A resposta à solução de problemas deverá ocorrer no prazo e condições especificados no Termo de Referência.

6.5. O fornecedor deve implantar a solução no tempo definido no Termo de Referência, a contar da assinatura do contrato.

6.6. Durante toda a vigência do contrato, a empresa vencedora do certame deverá garantir a atualização de versões de sistema operacional da plataforma, assim como da base de dados de segurança, por VIA ELETRÔNICA, bem como garantir a troca de hardware (RMA) juntamente com a fabricante, em caso de eventuais falhas de funcionamento, com SLA de 2 dias úteis para atendimento e entrega do equipamento objeto da troca.

6.7. O suporte técnico especializado, a ser prestado pela CONTRATADA, deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, em português, com disponibilidade para abertura de chamados ilimitados através de canais web, e-mail e/ou telefone.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. Atualmente o HFA possui em produção no ambiente de rede e proteção de dados, uma plataforma de NGFW, composta por Hardware e Softwares, da fabricante Palo Alto Networks, modelo **PA-3420**. Este equipamento está atuando como proteção de borda no ambiente do HFA. O objetivo deste processo é ampliar a proteção oferecida pelos firewalls de próxima geração

(NGFW) já implementados na borda da rede para a rede interna. A implementação de NGFWs adicionais para a segmentação e segurança da rede interna garantirá uma defesa robusta contra ameaças externas e internas, além de melhorar o monitoramento e controle do tráfego interno, com foco na proteção de dados sensíveis e em conformidade com políticas de segurança. Desta forma, é necessária a contratação de empresa especializada para fornecimento de Plataforma de Hardware e Softwares (subscrições/assinaturas) da fabricante Palo Alto Networks, modelo PA-1410, para integração da atual plataforma em produção no ambiente do HFA, com licenciamento, suporte e garantia pelo período de 36 (trinta e seis) meses e instalação completa.

7.2. A solução é composta por hardware, softwares e serviços, conforme a imagem abaixo, e ficha técnica anexo (7752173):

Feature	PA-1410
Performance	
*1. Firewall throughput measured with App-ID and User-ID features enabled utilizing AppMix transactions. 2. Threat prevention throughput measured with App-ID, User-ID, IPS, antivirus and anti-spyware features enabled utilizing AppMix transactions. 3. New sessions per second measured with 1 byte HTTP transactions. Additional	
, for VM models, please refer to hypervisor, cloud specific data sheet for associated performance.	
App-ID firewall throughput	8.5 Gbps
Threat prevention throughput	4.5 Gbps
IPSec VPN throughput	4.1 Gbps
Connections per second	100,000
Sessions	
Max sessions (IPv4 or IPv6)	945,000
Policies	
Security rules	5000
Security rule schedules	250
NAT rules	3,000
Decryption rules	750
App override rules	750
Tunnel content inspection rules	750
SD-WAN rules	400
Policy based forwarding rules	750
Captive portal rules	750
DoS protection rules	750
Security Zones	
Max security zones	150
Objects (addresses and services)	
Address objects	20,000
Address groups	2,000
Members per address group	2,500
Service objects	3,000
Service groups	1,500
Members per service group	1,500
FQDN address objects	2,048
Max DAG IP addresses	150,000
*System wide capacity	
Tags per IP address	32
Security Profiles	
Security profiles	150
App-ID	
Custom App-ID signatures	6,000
Shared custom App-IDs	512
Custom App-IDs (virtual system specific)	6,416
User-ID	
IP-User mappings (management plane)	512,000
IP-User mappings (data plane)	128,000
Active and unique groups used in policy	1,000
*Aggregate of LDAP groups, XML API Groups and Dynamic User Groups	
Number of User-ID agents	100
Monitored servers for User-ID	100
Terminal server agents	1,000
Tags per User	32
*Only valid for PAN-OS 9.1 and above	
SSL Decryption	
Max SSL inbound certificates	125
SSL certificate cache (forward proxy)	2,000
Max concurrent decryption sessions	51,200
Decryption Port Mirror	Yes
Network Packet Broker	No
*For VM-Series, check VM Flex Licensing on Customer Support Portal	
HSM Supported	Yes
URL Filtering	
Total entries for allow list, block list and custom categories	25,000
Max custom categories	2,849
Max custom categories (virtual system specific)	500
Dataplane cache size for URL filtering	200,000
Management plane dynamic cache size	600,000

EDL	
Max number of custom lists	30
Max number of IPs per system	50,000
Max number of DNS Domains per system	100,000
Max number of URL per system	100,000
Shortest check interval (min)	5
Interfaces	
Mgmt - out-of-band	10/100/1000, RJ45/ Micro USB console
Mgmt - 10/100/1000 high availability	2
Mgmt - 40Gbps high availability	NA
Mgmt - 10Gbps high availability	1
Traffic - 10/100/1000	8
Traffic - 10M/100M/1G/2.5G/5G	4
*10M/100M	
Traffic - 100/1000/10000	NA
Traffic - 10Gbps SFP	6
Traffic - 10Gbps SFP+	4
Traffic - 25Gbps SFP28	NA
Traffic - 40/100Gbps QSFP+/QSFP28	NA
IO2: 1q tags per device	4,094
IO2: 1q tags per physical interface	4,094
Max interfaces (logical and physical)	1,024
Maximum aggregate interfaces	10
Maximum SD-WAN virtual interfaces	1,000
Power Over Ethernet	
PoE Enabled Interfaces	4
PoE Interface Speed	1/2.5/5G
Total Power Budget	151 Watts
Max Power per single port	90 Watts
Cellular Interface	
5G	NA
Virtual Routers	
Virtual routers	10
Virtual Wires	
Virtual wires	1,024
Virtual Systems	

Base virtual systems	1
Max virtual systems	6
*Additional licenses are required for virtual system capacities above the base virtual systems capacity	
Routing	
IPv4 forwarding table size	10,000
*Entries shared across virtual routers	
IPv6 forwarding table size	5,000
*Entries shared across virtual routers	
System total forwarding table size	10,000
Max route maps per virtual router	50
Max routing peers (protocol dependent)	1,000
Static entries - DNS proxy	1,024
Bidirectional Forwarding Detection (BFD) Sessions	512
L2 Forwarding	
ARP table size per device	3,000
IPv6 neighbor table size	3,000
MAC table size per device	3,000
Max ARP entries per broadcast domain	3,000
Max MAC entries per broadcast domain	3,000
NAT	
Total NAT rule capacity	3,000
Max NAT rules (static)	3,000
*Configuring static NAT rules to full capacity requires that no other NAT rule types are used.	
Max NAT rules (DIP)	2,000
*Configuring DIP NAT rules to full capacity requires that no other NAT rule types are used.	
Max NAT rules (DIPP)	1,500
Max translated IPs (DIP)	128,000
Max translated IPs (DIPP)	1,500
*DIPP translated IP capacity is proportional to the DIPP pool oversubscription value. The capacity shown here is based on an oversubscription value of 1x.	
Default DIPP pool oversubscription	2
*Source IP and source port reuse across concurrent sessions	
Address Assignment	
DHCP servers	5
DHCP relays	500
*Maximum capacity represents total DHCP servers and DHCP relays combined	
Max number of assigned addresses	64,000
High Availability	
Devices supported	2
Max virtual addresses	48
QoS	
Number of QoS policies	2,000
Physical interfaces supporting QoS	12
Clear text nodes per physical interface	31
DSCP marking by policy	Yes
Subinterfaces supported	500
IPSec VPN	
Max IKE Peers	2,800
Site to site (with proxy id)	2,800
SD-WAN IPSec tunnels	2,800
GlobalProtect Client VPN	
Max tunnels (SSL, IPSec, and IKE with XAUTH)	1,500
GlobalProtect Clientless VPN	
Max SSL tunnels	200
Multicast	
Replication (egress interfaces)	500
Routes	2,000
Product Notes	
End-of-sale	NA

7.3. Considerando que o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, no cenário atual, o HFA possui solução modelo **PA-3420** protegendo a rede, acesso norte x sul (borda), e este projeto visa **expandir** este ambiente, com gerenciamento centralizado das regras e logs através do **PANORAMA CENTRAL MANAGEMENT**, para implementação de proteção lateral (rede interna).

7.4. É expressamente recomendado que sejam adicionados equipamentos do mesmo fabricante da Solução já em produção, com foco no Gerenciamento Centralizado através do **PANORAMA CENTRAL MANAGEMENT** , que é a Plataforma de Centralização de políticas, regras, análise de logs e relatoria da Palo Alto Networks, garantindo diversas vantagens para uma infraestrutura segurança coesa e unificada.

ITEM	OBJETO	MÉTRICA OU UNIDADE	QTD
1	Firewall Palo Alto Networks PA-1410 (PAN-PA-1410-AC) para proteção do ambiente interno, com licenciamento ATP (Advanced Threat Prevention), AWF (Advanced WildFire) e garantia da Fabricante para o período de 36 (trinta e seis) meses, incluindo todos os acessórios (8 x PAN-SFP-PLUS-SR), incluindo Instalação física e lógica e suporte	UN	2

Tabela 1 - Quantidade dos bens

8. Levantamento de soluções

8.1. DESCRIÇÃO DAS SOLUÇÕES TIC

8.1.1. Solução 1: Firewall UTM

8.1.1.1. Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

8.1.1.2. Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: <https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm>

8.1.2. Solução 2: Firewall de Próxima Geração

8.1.2.1. É uma plataforma de rede integrada baseada em inspeção profunda (deep packet inspection), provendo múltiplos mecanismos de proteção em um único equipamento, tais como Intrusion Prevention System (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação in-line sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, Stateful Inspection Protocol, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

8.1.2.2. Atualmente o HFA possui em produção no ambiente de rede e proteção de dados, uma plataforma de NGFW, composta por Hardware e Softwares, da fabricante Palo Alto Networks, modelo PA-3420. Este equipamento está atuando como proteção de borda no ambiente do HFA. O objetivo deste processo é ampliar a proteção oferecida pelos firewalls de próxima geração (NGFW) já implementados na borda da rede para a rede interna. A implementação de NGFWs adicionais para a segmentação e segurança da rede interna garantirá uma defesa robusta contra ameaças externas e internas, além de melhorar o monitoramento e controle do tráfego interno, com foco na proteção de dados sensíveis e em conformidade com políticas de segurança. Desta forma, é necessária a contratação de empresa especializada para fornecimento de Plataforma de Hardware e Softwares (subscrições/assinaturas) da fabricante Palo Alto Networks, modelo PA-1410, para integração da atual plataforma em produção no ambiente do HFA, com licenciamento, suporte e garantia pelo período de 36 (trinta e seis) meses e instalação completa.

Referência: <https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfw>

8.1.3. Solução 3: Composição de soluções de segurança

8.1.3.1. A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

8.1.3.2. Por contar com uma quantidade de funcionários reduzida para a administração da rede, o setor de segurança da informação dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao HFA. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

8.1.3.3. Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

8.1.3.4. Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

8.1.3.5. Solução 4: Solução de software livre

8.1.3.6. Não se aplica.

8.2. IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Descrição da solução (ou cenário)
1	Firewall UTM
2	Firewall de Próxima Geração
3	Composição de soluções de segurança

Tabela 2 - Identificação das Soluções

9. Análise comparativa de soluções

Segue análise:

Requisito	Solução	Sim	N
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X	
	Solução 2	X	
	Solução 3	X	
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		
	Solução 2		
	Solução 3		
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		
	Solução 2		
	Solução 3		
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1		
	Solução 2		
	Solução 3		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1		
	Solução 2		
	Solução 3		
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1		
	Solução 2		
	Solução 3		

Tabela 3 - Análise Comparativa das Soluções

10. Registro de soluções consideradas inviáveis**10.1. Solução 1: Firewall UTM**

10.1.1. Para atender as necessidades do HFA, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do HFA envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com

softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

10.1.2. Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

10.1.3. Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

10.1.4. E por fim, com o intuito de proteger os investimentos do HFA para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

10.2. Solução 3: Composição de soluções de segurança

10.2.1. A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

10.2.2. Por contar com um quantitativo reduzido de funcionários para a administração da rede, o DTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o HFA.

10.2.3. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

10.2.4. Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

10.2.5. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

10.2.6. Políticas de segurança podem ser aplicadas de forma inconsistente devido às diferenças entre as funcionalidades e interfaces dos fabricantes.

10.2.7. Inconsistências podem levar a vulnerabilidades, como brechas de segurança ou regras conflitantes.

10.2.8. A frequência de atualizações de firmware, patches e versões pode variar entre os fabricantes, o que pode complicar a manutenção da rede e abrir brechas de segurança em momentos de desatualização.

10.2.9. Soluções unificadas geralmente oferecem automações, como aplicação de políticas ou resposta a ameaças, enquanto equipamentos diferentes podem exigir intervenções manuais ou soluções de terceiros para automação.

10.3. Solução 4: Utilização de softwares livres

10.3.1. Não se aplica.

10.3.2. A opção por ferramentas livres em substituição aos softwares proprietários, além de implicar em treinamento dos usuários e perda de familiaridade com as ferramentas já utilizadas, traz outras consequências como a perda na utilização de funcionalidades especiais e mais complexas, tendo impacto na produtividade dos usuários, e em função do largo uso destes produtos no HFA, sua substituição por produtos que não mantenham compatibilidade nos formatos de arquivos, por exemplo, implicaria em vários arquivos com formatos diferentes que não se integram, gerando retrabalho e perda de produtividade. Programas similares, segundo os usuários, não possuem o mesmo workflow, o que dificulta a adaptação.

11. Análise comparativa de custos (TCO)

11.1. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

11.1.1. As estimativas, estabelecidas neste instrumento foram realizadas por pesquisa de preço constantes nos orçamentos '7784232', '7795496', '7795506' e '7795518'.

11.1.2. A análise dos serviços considerados (realização de licitação própria) pautou-se nos seguintes pontos:

11.1.2.1. Nas características técnicas essenciais para o atendimento das necessidades.

11.1.2.2. No atendimento aos requisitos mínimos especificados da **IN SGD/ME nº 94/2022**.

11.1.2.3. Na peculiaridades do HFA, em relação à aquisição da solução existente em alta disponibilidade, incluindo serviços técnicos de instalação, capacitação técnica, suporte técnico e garantia.

11.1.2.4. Os valores apresentados foram estimados baseando-se em ampla pesquisa de preços, onde foram obtidos a média dos preços.

11.2. CENÁRIO 1

11.2.1. Descrição: Solução 2: Firewall de Próxima Geração - Pesquisa de parâmetro I (Preços Públicos) - Solução de Next Generation Firewall

11.2.2. Para responder ao cenário digital atual, explanado mais abaixo, propomos a contratação de empresa especializada para fornecimento de solução de Next Generation Firewall (NGFW) da fabricante Palo Alto Networks, para proteção interna do HFA, incluindo licenciamento, suporte e garantia pelo período de 36 (trinta e seis) meses e serviço de implantação. Dentre as melhorias que poderão ser obtidas, podemos destacar:

- Gerenciamento da plataforma de segurança de rede, visando manter o controle das funcionalidades e regras em uma plataforma única, podendo ser acessado remotamente;

- Diminuição do risco operacional da Infraestrutura de TI;

- Aumento da eficiência de monitoração de eventos;

- Manutenção da proteção perimetral dos dados e sistemas atualmente em produção;

- Manutenção da disponibilidade das aplicações críticas atualmente em produção;

- Manutenção da solução atual de Next Generation Firewall em alta disponibilidade;

- As soluções de Next Generation Firewall integram diferentes tipos de proteção, tais como antivírus de perímetro, IPS (Sistema de Prevenção de Intrusão), firewall de camada de aplicação, filtro de navegação na Internet, entre outros, em um único equipamento, reduzindo o custo de manutenção e administração. Estas vêm sendo amplamente utilizadas por órgãos que precisam estar conectados de forma segura;

- Unificação da Plataforma de Gerenciamento: A utilização de uma única solução para toda a rede, tanto para a borda quanto para a rede interna, permite uma administração centralizada por meio de uma interface única. Isso simplifica a configuração, o monitoramento e a gestão das políticas de segurança, além de reduzir a complexidade administrativa;

- Visibilidade Abrangente: O gerenciamento centralizado possibilita uma visão integrada de toda a infraestrutura de segurança, facilitando a identificação de ameaças e a análise de eventos de segurança em tempo real. A partir de um único painel, é possível monitorar tanto a borda quanto a rede interna, garantindo um controle eficiente sobre o tráfego e a segurança da rede como um todo;

- Eficiência Operacional: Com a centralização das funções de administração, a equipe de TI ou de segurança da informação poderá aplicar configurações de políticas e regras de segurança de forma uniforme em toda a rede. Isso reduz a possibilidade de erros de configuração que podem ocorrer quando se utilizam diferentes soluções de fabricantes distintos;

- Automatização e Orquestração: Soluções do mesmo fabricante geralmente oferecem a integração de funcionalidades de automação e orquestração de segurança. A capacidade de automatizar a aplicação de políticas de segurança, responder a incidentes e realizar ações corretivas de forma coordenada torna o ambiente mais ágil e resiliente frente a ameaças.

- Manter a solução do mesmo fabricante em todo o ambiente de segurança, visando a compatibilidade da plataforma, garante integração total entre os dispositivos de NGFW existentes em produção e os novos, facilitando a operação de ambos. Isso se traduz em uma série de vantagens:

- Menor Risco de Incompatibilidade: Soluções de diferentes fabricantes podem apresentar problemas de interoperabilidade, exigindo customizações ou configurações complexas para garantir o funcionamento adequado em conjunto. Utilizando equipamentos do mesmo fabricante, elimina-se o risco de problemas relacionados à integração, garantindo um ambiente mais estável;

- Atualizações e Patches Consistentes: Quando se utiliza a mesma solução de NGFW, as atualizações de firmware, patches de segurança e novos recursos são implementados de forma coordenada em toda a infraestrutura, reduzindo o risco de vulnerabilidades de segurança em versões não compatíveis entre diferentes dispositivos;

- Continuidade e padronização tecnológica: Soluções de segurança frequentemente sofrem atualizações por descobertas de vulnerabilidades, a solução atual da fabricante Palo Alto Networks, vem funcionando nestes 3 anos totalmente a contento e está bem adaptada ao ambiente de Segurança da Informação do HFA, não havendo nada que desabone tanto esta fabricante, como a Plataforma de Segurança como um todo. É aconselhável a continuidade do uso de sua plataforma, assim como manutenção da garantia e suporte;

- Políticas de Segurança Padronizadas: A manutenção da mesma solução garante que as políticas de segurança aplicadas à borda da rede possam ser estendidas de maneira consistente para a rede interna. Isso ajuda na padronização das regras de firewall e da segmentação de rede, o que é fundamental para garantir a conformidade com as exigências de segurança e governança;

- Relatórios e Auditoria Simplificados: Com uma única solução em toda a rede, os relatórios de segurança e as auditorias podem ser gerados de forma mais eficiente, com dados consistentes e centralizados, o que facilita a elaboração de relatórios para auditorias internas e externas;

- Treinamento e Suporte: A equipe de TI e os administradores de segurança já estarão familiarizados com a interface, a configuração e os procedimentos de gerenciamento da solução existente. Isso elimina a necessidade de treinamento adicional para novas plataformas, além de reduzir os custos associados ao suporte técnico de diferentes fornecedores.

Item	Descrição	Pregão / UASG	Qtd	Valor Unitário	TOT
1	Equipamento Segurança Rede Aplicação: Firewall , Tipo: Appliance	NºPregão:90021/2024 UASG: 160482 1A. BRIGADA DE INFANTARIA DE SELVA/R	02	R\$465.000,00	R
1	Equipamento Segurança Rede Aplicação: Firewall , Tipo: Appliance	NºPregão:90167/2024 UASG: 254445 INSTITUTO DE TECNOLOGIA EM IMUNOBIOLOGICO	02	R\$ 430.000,00	R
1	Equipamento Segurança Rede Aplicação: Firewall , Tipo: Appliance	NºPregão:90036/2024 UASG: 155021 HOSPITAL DAS CLÍNICAS DE MINAS GERAIS	02	R\$ 477.000,00	R
1	Equipamento Segurança Rede Aplicação: Firewall , Tipo: Appliance	NºPregão:90008/2024 UASG: 154043 FUNDACAO UNIVERSIDADE FEDERAL DE UBERLANDIA	02	R\$ 582.548,00	R

Custo Total de Propriedade – Memória de Cálculo

Investimento Necessário:

Considerando a média de valor dos preços públicos consultados:

Item	Descrição	Métrica ou UN	Qtd	Valor Unitário	TOT.
1	Equipamento Segurança Rede Aplicação: Firewall , Tipo: Appliance	UN	02	R\$ 488.637,00	R\$

Média: 'ITEM 1' R\$488.637,00 (quatrocentos e oitenta e oito mil seiscentos e trinta e sete reais)

11.2.3. CENÁRIO 2

11.2.4. Descrição: Solução 2: Firewall de Próxima Geração - Pesquisa de parâmetro IV (Fornecedores) - Solução Paloalto

11.2.5. Aquisição por licitação própria de plataforma de Next Generation Firewall para alta disponibilidade.

Item	Descrição	Fornecedor	Métrica ou UN	Qtd	Valor Unitário	Total
1	Firewall Palo Alto Networks PA-1410 (PAN-PA-1410-AC) para proteção do ambiente interno, com licenciamento ATP (Advanced Threat Prevention), AWF (Advanced WildFire) e garantia da Fabricante para o período de 36 (trinta e seis) meses, incluindo todos os acessórios (8 x PAN-SFP-PLUS-SR), incluindo Instalação física e lógica e suporte.	2R DATATEL TELEINFORMÁTICA LTDA	UN	02	R\$ 453.900,00	R\$907.800,00

Item	Descrição	Fornecedor	Métrica ou UN	Qtd	Valor Unitário	Total
1	Firewall Palo Alto Networks PA-1410 (PAN-PA-1410-AC) para proteção do ambiente interno, com licenciamento ATP (Advanced Threat Prevention), AWF (Advanced WildFire) e garantia da Fabricante para o período de 36 (trinta e seis) meses, incluindo todos os acessórios (8 x PAN-SFP-PLUS-SR), incluindo Instalação física e lógica e suporte	APPROACH TECNOLOGIA LTDA	UN	02	R\$521.668,43	R\$1.043.336,86

Item	Descrição	Fornecedor	Métrica ou UN	Qtd	Valor Unitário	Total
1	Firewall Palo Alto Networks PA-1410 (PAN-PA-1410-AC) para proteção do ambiente interno, com licenciamento ATP (Advanced Threat Prevention), AWF (Advanced WildFire) e garantia da Fabricante para o período de 36 (trinta e seis) meses, incluindo todos os acessórios (8 x PAN-SFP-PLUS-SR), incluindo Instalação física e lógica e suporte	TDEC REDES DE COMPUTADORES LTDA	UN	02	R\$549.000,00	R\$1.098.000,00

Custo Total de Propriedade – Memória de Cálculo

Investimento Necessário:

Item	Descrição	Métrica ou UN	Qtd	Valor Unitário	Total
1	Firewall Palo Alto Networks PA-1410 (PAN-PA-1410-AC) para proteção do ambiente interno, com licenciamento ATP (Advanced Threat Prevention), AWF (Advanced WildFire) e garantia da Fabricante para o período de 36 (trinta e seis) meses, incluindo todos os acessórios (8 x PAN-SFP-PLUS-SR), incluindo Instalação física e lógica e suporte	UN	02	R\$ 508.189,47	R\$1.016.378,95

11.3. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

ITEM	NOME	Métrica ou UN	QNTD	MÉDIA CENÁRIO 1 e 2	
1	Firewall Palo Alto Networks PA-1410 (PAN-PA-1410-AC) para proteção do ambiente interno, com licenciamento ATP (Advanced Threat Prevention), AWF (Advanced WildFire) e garantia da Fabricante para o período de 36 (trinta e seis) meses, incluindo todos os acessórios (8 x PAN-SFP-PLUS-SR), incluindo Instalação física e lógica e suporte	UN	2	R\$497.016,63	1
TCO					R\$99

12. Descrição da solução de TIC a ser contratada

12.1. Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o HFA é a **Solução 2: Firewall de Próxima Geração**, mantendo a solução da mesma fabricante já instalada e em produção no ambiente de segurança da informação do HFA, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pelo departamento de segurança da informação.

13. Estimativa de custo total da contratação

Valor (R\$): 994.033,26

13.1. O valor total estimado para a contratação de empresa especializada para fornecimento de solução de Next Generation Firewall (NGFW) da fabricante Palo Alto Networks, para proteção interna do HFA, incluindo licenciamento, suporte e garantia pelo período de 36 (trinta e seis) meses e serviço de implantação, é de **R\$994.033,26** (novecentos e noventa e quatro mil trinta e três reais e vinte e seis centavos).

ITEM	DESCRIÇÃO	MÉTRICA OU UNIDADE	QTD	VALOR UNITÁRIO	
1	Firewall Palo Alto Networks PA-1410 (PAN-PA-1410-AC) para proteção do ambiente interno, com licenciamento ATP (Advanced Threat Prevention), AWF (Advanced WildFire) e garantia da Fabricante para o período de 36 (trinta e seis) meses, incluindo todos os acessórios (8 x PAN-SFP-PLUS-SR), incluindo Instalação física e lógica e suporte.	UN	02	R\$497.016,63	
TOTAL					R\$

13.2. Os valores constantes da tabela presente no item 7 do presente Estudo Técnico Preliminar foram obtidos com base na média dos preços da pesquisa inicial.

14. Justificativa técnica da escolha da solução

14.1. No ano de 2022 foi implantado no HFA, através do processo nº 60550.027671/2021-56 e contrato nº 37/2021-HFA, uma plataforma de Firewall de última geração com Appliance de alta performance, da Fabricante Palo Alto Networks, proporcionando um aumento substancial na segurança, desempenho e estabilidade no ambiente de rede, suportando a rede externa, aplicações críticas, sistemas, rede local (interna) e servidores;

14.2. Este equipamento foi utilizado em produção no ambiente como Firewall CORE até o ano de 2023;

14.3. Através do processo **60550.004467/2023-29**, foi implementada no HFA uma solução em alta disponibilidade, para proteção de borda, também da Fabricante Palo Alto Networks;

14.4. No cenário atual, o HFA possui solução modelo PA-3420 protegendo a borda da rede, acesso norte x sul (borda), e um equipamento PA-5220 para proteção interna;

14.5. Este equipamento tem seu fim de vida anunciado para o dia 31 de agosto de 2028, conforme link do fabricante: <https://www.paloaltonetworks.com/services/support/end-of-life-announcements/hardware-end-of-life-dates> e a partir desta data, não será mais possível renovar seu suporte e garantia, ou atualizar a base de dados e Sistema Operacional;

14.6. Este projeto visa complementar o ambiente de forma integrada, com gerenciamento centralizado das regras e logs através do PANORAMA CENTRAL MANAGEMENT, para implementação de proteção lateral (rede interna).

14.7. É expressamente recomendado que sejam adicionados equipamentos do mesmo fabricante da Solução já em produção, com foco no Gerenciamento Centralizado através do PANORAMA CENTRAL MANAGEMENT, que é a Plataforma de Centralização de políticas, regras, análise de logs e relatoria da Palo Alto Networks, garantindo diversas vantagens para uma infraestrutura segurança coesa e unificada.

14.8. A garantia do equipamento fornecida na aquisição oriunda do processo nº 60550.027671/2021-56, inclui um atendimento de suporte técnico prestado pela própria fabricante da solução, por telefone, de forma remota. Em casos específicos se faz necessário um suporte mais personalizado, com atendimento no local (onsite) para apoio à configuração lógica das regras e políticas e manutenção técnica em caso de falhas no equipamento (hardware).

14.9. Esta empresa será responsável por manter, juntamente com a equipe técnica do HFA, o ambiente de Segurança da Informação totalmente ativo, atualizado e com os equipamentos de Firewall em pleno funcionamento, atuando com as configurações indicadas nas melhores práticas de mercado.

14.10. Parcelamento da Solução de TIC Escolhida

14.10.1. O objeto da pretendida contratação, bem como a composição dos itens do escopo de fornecimento detalhado na estimativa da demanda, que formam o conjunto de bens e serviços a serem contratados, configuram uma única solução de Tecnologia da Informação.

14.10.2. Todos os itens de hardware e subscrições do escopo de fornecimento possuem correlação entre si e são elementos inseparáveis de uma mesma e única solução de Tecnologia da Informação para prover a infraestrutura desejada para a

manutenção da eficácia da solução de NGFW, para a solução de alta disponibilidade. Desta forma, os serviços desta contratação são INTERDEPENDENTES, formando solução única para o fornecimento da plataforma de NGFW em alta disponibilidade. Portanto, o objeto deverá ser contratado em grupo e fornecido por apenas uma única empresa especialista na solução técnica.

14.10.3. Neste caso tecnicamente não se faz viável o parcelamento da solução, pois a mesma empresa CONTRATADA que fornecer a plataforma de NGFW, deve possuir a capacidade técnica de realizar a implantação (instalação física e configuração lógica) e suportar tecnicamente a solução em alta disponibilidade, no ambiente do HFA.

14.10.4. Não justifica a elaboração de contratos em separado, assim como o gerenciamento operacional destes, para o fornecimento da plataforma de NGFW e prestação de serviços de implantação, configuração e suporte desta plataforma, durante todo o período contratado.

14.10.5. Por fim, o agrupamento de todos os itens deste processo visa garantir a otimização dos prazos de execução, viabilizando a sincronia nos fornecimentos e serviços de instalações e treinamento, evitando assim que um fornecedor venha a prejudicar a execução de outro.

15. Justificativa econômica da escolha da solução

15.1. A contratação pretendida visa prover a plena capacidade e disponibilidade do ambiente de rede e segurança da informação do HFA, propiciando a necessária estruturação de segurança tecnológica nesses sistemas, infraestruturas de TI, mantendo integral proteção, operação e criticidade, essenciais para as atividades finalísticas e que são sensíveis a graves ameaças (disseminação de ataques) e distúrbios de toda natureza que podem provocar panes, resultando em graves prejuízos a Administração.

15.2. O HFA ganha em capacidade de gestão do contrato, com instrumentos de cobrança efetiva, e com procedimentos padronizados de suporte técnico durante o período de licenciamento e garantia, propiciando agilidade na identificação e resolução dos problemas advindos de falhas ou outros eventos que estejam relacionados ao item 01, que funcionarão interligados.

16. Benefícios a serem alcançados com a contratação

16.1. É expressamente recomendado que sejam adicionados equipamentos do mesmo fabricante da Solução já em produção, com foco no Gerenciamento Centralizado através do PANORAMA CENTRAL MANAGEMENT, que é a Plataforma de Centralização de políticas, regras, análise de logs e relatoria da Palo Alto Networks, garantindo diversas vantagens para uma infraestrutura segurança coesa e unificada. Com isso, os seguintes benefícios para um gerenciamento centralizado são garantidos:

16.2. Unificação da Plataforma de Gerenciamento: A utilização de uma única solução para toda a rede, tanto para a borda quanto para a rede interna, permite uma administração centralizada por meio de uma interface única. Isso simplifica a configuração, o monitoramento e a gestão das políticas de segurança, além de reduzir a complexidade administrativa;

16.3. Visibilidade Abrangente: O gerenciamento centralizado possibilita uma visão integrada de toda a infraestrutura de segurança, facilitando a identificação de ameaças e a análise de eventos de segurança em tempo real. A partir de um único painel, é possível monitorar tanto a borda quanto a rede interna, garantindo um controle eficiente sobre o tráfego e a segurança da rede como um todo;

16.4. Eficiência Operacional: Com a centralização das funções de administração, a equipe de TI ou de segurança da informação poderá aplicar configurações de políticas e regras de segurança de forma uniforme em toda a rede. Isso reduz a possibilidade de erros de configuração que podem ocorrer quando se utilizam diferentes soluções de fabricantes distintos;

16.5. Automação e Orquestração: Soluções do mesmo fabricante geralmente oferecem a integração de funcionalidades de automação e orquestração de segurança. A capacidade de automatizar a aplicação de políticas de segurança, responder a incidentes e realizar ações corretivas de forma coordenada torna o ambiente mais ágil e resiliente frente a ameaças.

16.6. Manter a solução do mesmo fabricante em todo o ambiente de segurança, visando a compatibilidade da plataforma, garante integração total entre os dispositivos de NGFW existentes em produção e os novos, facilitando a operação de ambos. Isso se traduz em uma série de vantagens:

16.7. Menor Risco de Incompatibilidade: Soluções de diferentes fabricantes podem apresentar problemas de interoperabilidade, exigindo customizações ou configurações complexas para garantir o funcionamento adequado em conjunto. Utilizando equipamentos do mesmo fabricante, elimina-se o risco de problemas relacionados à integração, garantindo um ambiente mais estável;

16.8. Atualizações e Patches Consistentes: Quando se utiliza a mesma solução de NGFW, as atualizações de firmware, patches de segurança e novos recursos são implementados de forma coordenada em toda a infraestrutura, reduzindo o risco de vulnerabilidades de segurança em versões não compatíveis entre diferentes dispositivos;

16.9. Continuidade e padronização tecnológica: Soluções de segurança frequentemente sofrem atualizações por descobertas de vulnerabilidades, a solução atual da fabricante Palo Alto Networks, vem funcionando nestes 3 anos totalmente a contento e está bem adaptada ao ambiente de Segurança da Informação do HFA, não havendo nada que desabone tanto esta fabricante, como a Plataforma de Segurança como um todo. É aconselhável a continuidade do uso de sua plataforma, assim como manutenção da garantia e suporte;

16.10. Políticas de Segurança Padronizadas: A manutenção da mesma solução garante que as políticas de segurança aplicadas à borda da rede possam ser estendidas de maneira consistente para a rede interna. Isso ajuda na padronização das regras de firewall e da segmentação de rede, o que é fundamental para garantir a conformidade com as exigências de segurança e governança;

16.11. Relatórios e Auditoria Simplificados: Com uma única solução em toda a rede, os relatórios de segurança e as auditorias podem ser gerados de forma mais eficiente, com dados consistentes e centralizados, o que facilita a elaboração de relatórios para auditorias internas e externas;

16.12. Treinamento e Suporte: A equipe de TI e os administradores de segurança já estarão familiarizados com a interface, a configuração e os procedimentos de gerenciamento da solução existente. Isso elimina a necessidade de treinamento adicional para novas plataformas, além de reduzir os custos associados ao suporte técnico de diferentes fornecedores.

16.13. A escolha de manter solução de NGFW do mesmo fabricante para a proteção da rede interna, além de garantir um gerenciamento centralizado eficiente, traz vantagens estratégicas significativas, como a unificação da plataforma de segurança, a facilidade de integração e a consistência operacional. Além disso, essa abordagem contribui para a redução de custos, melhora a conformidade com regulamentos de segurança e oferece maior previsibilidade quanto ao suporte e à evolução das soluções implementadas. Dessa forma, é recomendada a inclusão dessa condição no edital, com o intuito de preservar a eficiência, a segurança e a continuidade operacional da infraestrutura de TI.

16.14. Manutenção da solução atual de Next Generation Firewall em alta disponibilidade.

17. Providências a serem Adotadas

17.1. Não existem providências a serem adotadas pela administração previamente à celebração do contrato.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

18.1. Solução 2: Firewall de Próxima Geração

18.1.1. Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, tendo em vista o alto volume de tráfego do hospital, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises específicas.

18.1.2. A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

18.1.3. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

18.1.4. Requisitos Ambientais: Definem requisitos que a solução de TIC deve atender para estar em conformidade ao meio ambiente, como limites de emissão sonora de equipamentos, espaço máximo que deverá ocupar, descarte sustentável de resíduos, dentre outros que se apliquem. É necessário observar entre outros o menor impacto sobre recursos naturais como flora fauna, ar, solo e água; preferência para materiais, tecnologias e matérias-primas de origem local; maior eficiência na utilização de recursos

naturais como água e energia; maior geração de empregos, preferencialmente com mão de obra local; maior vida útil e menor custo de manutenção do bem e da obra; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens, serviços e obras. A área técnica consultou a Instrução Normativa nº 01/2010-SLTI/MPOG, o Decreto nº 7.746/2012, o Guia Nacional de Licitações Sustentáveis da AGU - 4ª Edição Agosto/2021 para verificar se os bens comuns a serem adquiridos integram, ou não, a lista de objetos regidos por disposições normativas de caráter ambiental, não constatando critérios de aplicabilidade no referido guia.

18.1.5. Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;

18.1.6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;

18.1.7. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.

18.1.8. Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.

18.1.9. Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;

18.1.10. Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);

18.1.11. Melhor filtro de conteúdo URL, sancionando acesso a sites indesejados de conteúdo ilícito; 18.1.12. Utilização do recurso de túneis VPN criptografados para comunicação e acesso as informações de forma segura por parte dos colaboradores do HFA a partir de suas residências;

19. 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](#).

MARCO ANTONIO DE SOUZA FARIAS

INTEGRANTE REQUISITANTE



Assinou eletronicamente em 11/06/2025 às 10:56:42.

FRANKLIN SOARES DE BRITO

INTEGRANTE TÉCNICO



Assinou eletronicamente em 11/06/2025 às 10:46:38.

ALESSANDRO DE SA BARBOSA

AUTORIDADE MÁXIMA DA ÁREA DE TIC



Assinou eletronicamente em 12/06/2025 às 13:03:27.