

Estudo Técnico Preliminar 721/2024

1. Informações Básicas

Número do processo: 23534.004043/2024-17

2. Descrição da necessidade

O presente Estudo Técnico Preliminar tem por objetivo de analisar viabilidade técnica e econômica para renovação de licenças e suporte técnico da solução de segurança atualmente em operação no Hospital Universitário Professor Edgard Santos - HUPES /UFBA com vistas a preservar a confidencialidade, integridade e disponibilidade das informações trafegadas na rede de dados do hospital.

Este ETP será classificado como Documento Público (não-sigiloso)

3. Necessidades de Negócio

Prover camadas de proteção cibernética, durante o período de licenciamento, minimizando riscos com invasões ou tentativas de ataques;

Garantir a segurança das informações do negócio e continuidade dos serviços de TIC.

Possibilitar mecanismos avançados de proteção tornando o ambiente mais seguro contra vulnerabilidades;

O software deve ser fornecido em caráter de licenciamento com atualizações e manutenções, bem como suporte ao hardware, incluindo troca de equipamento ou de peças;

Prover análise de logs(syslog) com geração de relatórios otimizados e customizados;

Prestação de suporte técnico na modalidade 24 X 7.

Comunicação entre a CONTRATADA e o fabricante, em casos de manutenção solicitada pelo CONTRATANTE, de forma que as informações tramitadas deverão transitar de forma segura, utilizando, sempre que possível, mecanismos de criptografia.

4. Área requisitante

Área Requisitante	Responsável
Setor de Tecnologia da Informação e Saúde Digital	Alexandre Jesus de Souza

5. Necessidades Tecnológicas

Renovação de licenças e suporte técnico da solução de segurança atualmente em operação no Hospital Universitário Professor Edgard Santos - HUPES/UFBA com vistas a preservar a confidencialidade, integridade e disponibilidade das informações trafegadas na rede de dados do hospital.

As licenças devem contemplar:

- a) Filtro de Botnet;
- b) Gateway Antivírus/Anti-Spyware/Intrusion Prevention/App Control/App Visualization;

- c) Filtragem de Conteúdo;
- d) Proteção contra ameaças avançadas e ameaças de Zero Day;
- e) Atualização de Software e Firmware;
- f) Garantia de Hardware;
- g) Suporte técnico em regime 24x7 do fabricante;
- h) Análise de Syslog com geração de relatórios otimizados e customizados;

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

Requisitos de Garantia, Manutenção e Assistência Técnica

- A garantia de funcionamento das licenças adquiridas, bem como o suporte técnico serão pelo período mínimo de 12 (doze) meses.
- O serviço de assistência técnica em GARANTIA deverá cobrir todos os procedimentos técnicos destinados ao reparo de eventuais falhas apresentadas nos equipamentos, de modo a restabelecer seu normal estado de uso e dentre os quais se incluem a substituição de peças, ajustes e reparos técnicos em conformidade com manuais e normas técnicas especificadas pelo fabricante.
- Durante o prazo de garantia será substituída sem ônus para o CONTRATANTE, a parte ou peça defeituosa, após a conclusão do respectivo analista de atendimento de que há a necessidade de substituir uma peça ou recolocá-la no sistema;
- Para efeitos de certificar a garantia, a CONTRATADA deve possuir recurso disponibilizado via web, site do próprio fabricante, que permita verificar a garantia do equipamento através da inserção do seu número de série;
- A substituição de componentes ou peças decorrentes da garantia não gera quaisquer ônus para o CONTRATANTE. Toda e qualquer peça ou componente consertado ou substituído, fica automaticamente garantido até o final do prazo de garantia técnica do contrato;
- Os serviços de suporte técnico abrangem:
 - Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;
 - Elaboração de relatórios, estudos e diagnósticos sobre o ambiente;
 - Transferência de conhecimento aos técnicos da CONTRATANTE referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes;
 - Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.
 - O suporte técnico contempla o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução.
 - O suporte técnico deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TIC (sistemas operacionais, servidores de banco de dados, servidores de aplicação etc.) necessários ao funcionamento da solução;
 - Deve contemplar também a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e release, será disponibilizada em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de patch de correção, a CONTRATADA deverá comunicar o fato ao CONTRATANTE e indicar a forma de obtenção e os defeitos que serão corrigidos pelo patch. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 (trinta) dias, a contar do lançamento de nova versão ou solução de correção;
 - A CONTRATADA será responsável pelos serviços de implantação das novas versões e releases dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos patches de correção e pacotes de serviço (service packs) relativos a esses produtos. Para a implantação das novas versões

//releases, bem como para a aplicação dos patches, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na CONTRATANTE;

- Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela CONTRATADA e /ou pelo fabricante; e através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução CONTRATADA;
- As peças substitutas deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento e devem integrar a garantia da solução;
- A CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, caso seja necessário, ao
- O atendimento deve ser 24x7x365, ou seja, 24 (vinte e quatro) horas por dia em 7 (sete) dias da semana por 365 (trezentos e sessenta e cinco) dias por ano, em língua portuguesa;

Requisitos Temporais

- O prazo para a CONTRATADA realizar o atendimento dos chamados de garantia técnica assistencial (atividades que incluem, mas não se limitam à execução e provimento de informação; assistência e orientação para: instalação, desinstalação, configuração, substituição e atualização de programas (software) e dispositivos físicos (hardware); aplicação de correções (patches) e atualizações de software; diagnósticos, avaliações e resolução de problemas; ajustes finos e customização da solução; esclarecimento acerca das características dos produtos e demais atividades. Durante a vigência do contrato, a CONTRATADA deverá prestar garantia técnica assistencial sempre que acionada pela CONTRATANTE.) será de 1 dia útil, após acionamento pela CONTRATANTE;
- O prazo para a CONTRATADA realizar o atendimento dos chamados de garantia técnica corretiva(série de procedimentos executados para recolocar a solução em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, ajustes, reparos e demais serviços necessários. Durante a vigência do contrato, a CONTRATADA deverá prestar garantia técnica corretiva sempre que acionada pela CONTRATANTE) será de:
 - Uma hora(1h) para chamadas de prioridade 1(P1), quatro horas(4h) para chamadas de prioridade, 2(P2), um dia útil (1 dia útil) para chamadas de prioridade 3(P3), após acionamento pela CONTRATANTE, conforme abaixo:

a) Prioridade 1(P1): Há um impacto crítico nas operações de negócios da CONTRATANTE;

b) Prioridade 2(P2): Aspectos significativos da operação de negócios da CONTRATANTE são impactados negativamente; a CONTRATANTE é capaz de executar operações de negócios, mas o desempenho das operações de negócios é degradado ou severamente limitado;

c) Prioridade 3(P3): São falhas que têm impacto limitado nas operações de negócios, enquanto a maioria das operações de negócios permanece funcional;

Requisitos de Segurança da informação

- Disponibilidade de funcionamento total da solução de firewall;
- Impor ações que evitem vazamento de dados e fraudes digitais relativos aos dados desse hospital e dos seus funcionários e usuários;
- Orientar e exigindo sigilo dos seus funcionários que venham a ter acesso aos dados do Hupes;
- Assegurar a gestão e tratamento de incidentes de forma sistematizada;

Crítérios e Práticas de Sustentabilidade

A contratação de serviços que envolve garantia e suporte a hardware e software deve estar alinhada aos princípios da sustentabilidade, conforme previsto na Lei nº 14.133/2021 e nos guias nacionais de contratações sustentáveis. Assim, são estabelecidos os seguintes critérios e práticas sustentáveis a serem considerados na presente contratação:

- **Crítérios Ambientais**
 - Adotar suporte técnico remoto sempre que possível, reduzindo deslocamentos e emissões de carbono associadas ao transporte de técnicos e equipamentos.
 - Otimizar o uso da energia elétrica, priorizando equipamentos e servidores com certificações de eficiência energética, como ENERGY STAR ou equivalentes.

- Utilizar infraestrutura de TI baseada em nuvem, minimizando a necessidade de hardware físico e reduzindo o consumo de materiais.
- Gerenciar corretamente os resíduos eletrônicos, garantindo a logística reversa para descarte responsável de peças e equipamentos substituídos, em conformidade com a Lei nº 12.305/2010 (Política Nacional de Resíduos Sólidos).
- Reduzir o uso de papel, garantindo que toda a documentação do serviço seja mantida em formato digital e incentivando processos paperless.
- **Critérios Sociais**
 - Condições de Trabalho Dignas: Exigir que a empresa contratada siga a legislação trabalhista vigente, garantindo segurança, saúde e bem-estar aos seus colaboradores.
 - Promoção de políticas de diversidade: Assegura equidade de oportunidades para mulheres, pessoas com deficiência e outros grupos historicamente sub-representados no mercado de trabalho.
 - Treinamento e Capacitação: Estimular programas de capacitação para os funcionários envolvidos na execução do contrato, promovendo conhecimento sobre práticas sustentáveis e eficiência operacional.
- **Critérios Econômicos**
 - Custo-Benefício Sustentável: Avaliação da proposta levando em consideração não apenas o menor preço, mas também os impactos ambientais e sociais das soluções oferecidas.
 - Redução de custos com infraestrutura física: Priorizar o suporte remoto e serviços que reduzam a utilização de equipamentos, promovendo eficiência operacional e redução de desperdícios.
 - Adoção de práticas de economia circular: Assegurar que peças e componentes sejam reaproveitados, reciclados ou descartados adequadamente.
- **Gestão Sustentável do Contrato**
 - Monitoramento e Auditoria: Implementação de indicadores de desempenho ambiental e social na execução do contrato, permitindo o acompanhamento das metas sustentáveis estabelecidas.
 - Redução da Pegada de Carbono: Preferência por fornecedores que possuam programas de compensação ambiental, como neutralização de emissões de carbono relacionadas à prestação do serviço.
 - Uso Racional de Recursos: Adoção de práticas que minimizem o consumo de papel, energia elétrica e água, estimulando o uso de meios digitais para comunicação e suporte técnico.

7. Estimativa da demanda - quantidade de bens e serviços

O HUPES necessita da renovação das licenças e suporte técnico da solução de segurança compatíveis com os equipamentos atualmente em produção - Firewall SonicWall Nsa 6650 (com HA - High Availability).

CATSER	DESCRIÇÃO	QUANTIDADE
27464	SonicWall Advanced Gateway Security Suite Bundle para firewall NSA 6650 por 12 meses. Ref: 01-SSC-8761	01
27464	SonicWall Analytics Software para firewall SonicWall NSA 6650 por 12 meses. Ref: 02-SSC-3951	01

8. Levantamento de soluções

Durante o levantamento realizado, foram identificadas 03(três) possibilidades :

Id	Descrição da solução (ou cenário)
1	Renovação das licenças, garantia e suporte técnico da solução de segurança atualmente em operação no HUPES
2	Aquisição de nova Solução de Firewall
3	Adoção de solução baseada em software livre

9. Análise comparativa de soluções

A Análise Comparativa de Soluções, deve considerar, além do aspecto econômico, os aspectos qualitativos em termo de benefícios para o alcance da contratação, de acordo com o objeto em estudo.

Solução 1 - Renovação das licenças e suporte técnico da solução de segurança atualmente em operação no HUPES

A solução de firewall atualmente utilizada no Hospital Universitário Professor Edgard Santos (HUPES) é do tipo Unified Threat Management (UTM), fornecida pela SonicWall. Composta por hardware e software, essa solução integra diversas funcionalidades de segurança, como prevenção contra intrusões, filtro de conteúdo, antivírus, antispymware, proteção contra ameaças e análise de logs com relatórios, entre outras. Sendo uma solução proprietária da SonicWall, seu funcionamento efetivo exige licenciamento específico, o que impede a interoperabilidade de licenças entre fabricantes, uma vez que cada fornecedor desenvolve seus equipamentos e licenças específicas.

No HUPES, a versão da licença é a Advanced Gateway Security Suite (AGSS) e o Analytics Software, aplicáveis ao equipamento NSa 6650. Esse pacote de segurança oferece análise de logs com relatórios e proteção avançada contra ameaças, incluindo ataques de “zero-day” — ataques que exploram vulnerabilidades no mesmo dia em que são descobertas e, portanto, ainda não possuem assinaturas de bloqueio.

Entre os pontos positivos dessa solução, destaca-se a preservação do investimento já realizado na solução, na experiência da equipe de TI com a ferramenta, e a constatação de que a solução atual ainda atende às demandas do hospital, sem necessidade de readequações na infraestrutura de rede.

Como pontos negativos, deve-se considerar que, adquiridos em 2021, os equipamentos podem demandar manutenções corretivas mais frequentes, potencialmente ocasionando interrupções.

Solução 2 - Aquisição de nova Solução de Firewall

Esta opção consiste na substituição da solução de segurança atual por meio da aquisição de novos equipamentos de firewall, com licenças, garantia e suporte técnico incluídos.

Entre os benefícios dessa opção, destacam-se o desempenho aprimorado e as novas funcionalidades que as soluções mais modernas oferecem. Firewalls de última geração proporcionam inspeção de tráfego mais eficiente, inteligência artificial para detecção e resposta a ameaças, além de funcionalidades avançadas para VPN e controle de acesso. Equipamentos novos são projetados para enfrentar ameaças emergentes, como ataques de *malware* avançados e *ransomware*, com maior eficiência, mitigando riscos que firewalls mais antigos podem não reconhecer adequadamente.

A aquisição de novos equipamentos incluirá licenças e garantia de suporte técnico, garantindo assistência especializada em caso de falhas ou incidentes, além de acesso a atualizações frequentes de segurança.

Entre os principais pontos negativos da aquisição de uma nova solução de firewall está a necessidade de parada técnica para sua implantação, o que pode impactar temporariamente a operação do HUPES. Além disso, essa mudança envolve custos adicionais associados ao processo de implantação e treinamento da equipe de TI.

Solução 3 - Adoção de solução baseada em software livre

A solução baseada em software livre consiste na utilização de solução de firewall baseada em software livre. Sendo a vantagem econômica um dos principais atrativos, já que em princípio não haveria custos diretos com licenciamento associados a soluções de software livre. Porém, firewalls baseados neste tipo de modelo podem não oferecer o mesmo nível de eficiência de segurança cibernética em comparação com soluções comerciais. Elas podem ser mais suscetíveis a ataques avançados e podem não fornecer recursos de proteção mais avançados e escaláveis. Além dessas dificuldades, o volume de tráfego de rede vem crescendo a cada ano exigindo hardwares dedicados para essa função. Assim, esta opção está aos poucos sendo substituída por ferramentas pagas com suporte, gerenciamento simplificado e garantia de funcionamento.

Segue avaliação das soluções, conforme determina o Inciso II do Art. 11 da IN 94/2022:

Requisito	ID da Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1 a 3	X		
A Solução está disponível no Portal do Software Público Brasileiro?				X
A Solução é um software livre ou software público?				X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?				X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)				X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)				X

10. Registro de soluções consideradas inviáveis

Solução 3 - Adoção de solução baseada em software livre

A solução baseada em software livre mostrou-se inviável, pois geralmente essas soluções não possuem o mesmo nível de eficiência de segurança cibernética, suporte técnico especializado, recursos avançados como filtragem de conteúdo ou detecção de ameaças sofisticadas em comparação com as soluções comerciais.

11. Análise comparativa de custos (TCO)

Em observação ao disposto no inciso VI do art. 28 do RLCE, a estimativa preliminar do valor da contratação, acompanhada dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte constam no processo SEI nº 23534.005299/2025-22.

12. Estimativa de custo total da contratação

[Conteúdo Sigiloso | Justificativa: A estimativa do valor da contratação encontra-se apartada do Estudo Técnico Preliminar, no Processo: 23534.0005188/2025-16, de modo a atender o REGULAMENTO DE LICITAÇÕES E CONTRATOS DA EBSEH, que traz em seu Art. 7 a respectiva orientação: Art. 7º O valor estimado do procedimento licitatório será sigiloso, sem prejuízo da divulgação do detalhamento dos quantitativos e das demais informações necessárias para a elaboração das propostas, facultando-se sua publicidade, mediante justificativa.]

13. Descrição da solução de TIC a ser contratada

Renovação das licenças SonicWall Advanced Gateway Security Suite (AGSS), com suporte técnico e garantia do *appliance* de firewall NSA 6650 (com HA - High Availability) e SonicWall Analytics Software pelo período de 12 meses.

As licenças devem contemplar:

- Filtro de Botnet;
- Gateway Antivírus/Anti-Spyware/Intrusion Prevention/App Control/App Visualization;
- Filtragem de Conteúdo;
- Proteção contra ameaças avançadas e ameaças de Zero Day;
- Atualização de Software e Firmware;

- f) Garantia de *Hardware*;
- g) Suporte em regime 24x7 do fabricante;
- h) Análise de Syslog com geração de relatórios otimizados e customizados;

Obs. Utilização das licenças tanto no equipamento principal SonicWall NSA 6650 (Serial Number: 2CB8ED2E2000), quanto no equipamento de redundância, SonicWall NSA 6650 (Serial Number: 2CB8ED2E1780), destinado à solução de alta disponibilidade (HA - *High Availability*).

14. Justificativa técnica da escolha da solução

Considera-se tecnicamente viável a Solução 01, sendo que o equipamento existente no HUPES atende as demandas de requisitos funcionais, processamento, desempenho, alta disponibilidade e segurança de rede. Com a renovação das licenças do firewall e software de análise a solução consegue operar de forma completa provendo a segurança necessária na borda da rede.

15. Justificativa econômica da escolha da solução

Conforme demonstrado no item 11 – Análise Comparativa de Custos (TCO), a Solução 1 apresenta o melhor custo-benefício, pois assegura a continuidade do serviço após os anos iniciais, preservando o investimento realizado. A adoção de uma nova solução acarretaria custos adicionais significativos, incluindo despesas com implantação, treinamento da equipe, aquisição de dispositivos complementares e, possivelmente, um período de indisponibilidade que poderia impactar os serviços prestados pelo HUPES.

Por outro lado, a renovação das licenças, do suporte e da garantia dos equipamentos existentes permite evitar esses custos e interrupções, garantindo a continuidade operacional, a eficiência dos serviços e o alinhamento com as melhores práticas de gestão de recursos, bem como com os objetivos de segurança e eficiência do HUPES.

16. Possíveis impactos ambientais

A contratação pode gerar os impactos ambientais elencados abaixo:

- Consumo excessivo de energia, aumentando emissões de CO devido ao uso contínuo de servidores e equipamentos.
- Geração de resíduos eletrônicos, com descarte inadequado de hardware obsoleto, baterias e cabos.
- Uso excessivo de insumos, como papel para relatórios e plástico para embalagem de equipamentos.
- Emissões de carbono por deslocamentos, devido a atendimentos presenciais frequentes.
- Contaminação ambiental por substâncias químicas, presentes em componentes eletrônicos.

Medidas de tratamento ou de mitigação dos possíveis impactos ambientais

- Adotar suporte técnico remoto sempre que possível, reduzindo deslocamentos e emissões de carbono associadas ao transporte de técnicos e equipamentos.

- Otimizar o uso da energia elétrica, priorizando equipamentos e servidores com certificações de eficiência energética, como ENERGY STAR ou equivalentes.
- Utilizar infraestrutura de TI baseada em nuvem, minimizando a necessidade de hardware físico e reduzindo o consumo de materiais.
- Gerenciar corretamente os resíduos eletrônicos, garantindo a logística reversa para descarte responsável de peças e equipamentos substituídos, em conformidade com a Lei nº 12.305/2010 (Política Nacional de Resíduos Sólidos).
- Reduzir o uso de papel, garantindo que toda a documentação do serviço seja mantida em formato digital e incentivando processos paperless.

17. Benefícios a serem alcançados com a contratação

A renovação do ciclo de licenças é essencial para garantir a segurança contínua da infraestrutura no Hospital Universitário Professor Edgard Santos (HUPES). Isso é fundamental para manter a confidencialidade, integridade e disponibilidade das informações transmitidas na rede de dados do hospital.

A falta de licenciamento da solução de segurança (firewall) pode representar um sério risco para a segurança das informações que circulam na rede. Isso pode resultar em quedas de desempenho nos acessos à rede, além de expor toda a rede de dados à infecção por *malwares*, como vírus, cavalos de tróia, *spywares*, ataques de *hackers* e outras ameaças virtuais. Portanto, é crucial priorizar a renovação das licenças para garantir a proteção adequada dos sistemas e dos dados do hospital.

18. Providências a serem Adotadas

Todas as providências cabíveis, como capacitação de servidores e adequação da infraestrutura já foram realizados, já que esta contratação é apenas da licença de uso, motivo pelo qual se dispensa quaisquer demais providências.

19. Declaração de Viabilidade

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

19.1. Justificativa da Viabilidade

O estudo preliminar demonstrou que a solução de segurança (firewall) atualmente em produção no HUPES não apenas continua atendendo à demanda, mas também se mantém como um mecanismo essencial para a proteção dos pilares da segurança da informação: confidencialidade, integridade e disponibilidade dos dados trafegados na rede. A ausência do devido licenciamento comprometeria o suporte, a garantia e a aplicação das atualizações mais recentes de assinaturas e proteções, expondo o hospital a ameaças digitais em constante evolução.

Além disso, a solução escolhida se mostra eficiente, adequada e alinhada às diretrizes gerenciais, demonstrando razoabilidade ao viabilizar a renovação das licenças, suporte e garantia. Essa decisão está fundamentada nos princípios da economicidade, transparência e eficiência, essenciais às contratações públicas, garantindo a continuidade e a segurança dos serviços prestados pelo HUPES.

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](#).

CARLOS EDUARDO LIMA PACHECO

Membro da comissão de contratação



Assinou eletronicamente em 20/03/2025 às 14:41:49.

JOANDERSON OLIVEIRA LEDO

Membro da comissão de contratação



Assinou eletronicamente em 20/03/2025 às 15:06:24.