FUNDAÇÃO UNIVERSIDADE FEDERAL DO ABC

Estudo Técnico Preliminar 91/2026

1. Informações Básicas

Número do processo: 23006.006809/2026-38

2. Descrição da necessidade

A necessidade consiste em viabilizar o teletrabalho e demais atividades de ensino, pesquisa e extensão que demandam acesso remoto seguro à rede da UFABC. Atualmente, o software de VPN opera em servidores genéricos (hardware Commercial Off-The-Shelf) que não possuem aceleração específica para criptografia, o que gera um gargalo de performance e impede a expansão do serviço para toda a universidade. A contratação visa a expansão da infraestrutura para entregar uma solução de alta performance e disponibilidade à comunidade acadêmica.

3. Área requisitante

Área Requisitante	Responsável
Núcleo de Tecnologia da Informação	Carlos Alberto Orsolon Silva

4. Necessidades de Negócio

Necessidade 1: Expansão da capacidade de acesso remoto seguro

Funcionalidade: Suportar o tráfego de acesso remoto à instituição com alto throughput (desempenho) de criptografia, eliminando as limitações do hardware atual.

Envolvidos: Comunidade estudantil, docentes, técnicos-administrativos e gestores do NTI.

Necessidade 2: Garantia de continuidade e alta disponibilidade do serviço.

Funcionalidade: Prover redundância física através de um cluster de dois equipamentos com fontes de alimentação redundantes (hot-swappable), garantindo que falhas de hardware não interrompam as atividades de teletrabalho e demais atividades de ensino, pesquisa e extensão

Envolvidos: Servidores em regime de PGD (Programa de Gestão e Desempenho) e equipe de infraestrutura de rede.

Necessidade 3: Segurança e conformidade tecnológica.

Funcionalidade: Aceleração de hardware para operações de VPN (como Intel QAT ou AVX-512) para reduzir a sobrecarga de CPU e aumentar a segurança nas conexões remotas.

Envolvidos: Núcleo de Tecnologia da Informação (NTI) e usuários externos que acessam dados sensíveis.

5. Necessidades Tecnológicas

A solução deve integrar-se ao ambiente computacional da UFABC, atendendo aos seguintes padrões e capacidades:

Arquitetura de Processamento: Necessidade de hardware com suporte nativo a instruções de aceleração criptográfica (como Intel QAT ou AVX-512) para processar altos volumes de tráfego VPN sem sobrecarga da CPU principal.

Capacidade de Throughput: O hardware deve suportar o desempenho esperado para a expansão institucional, com capacidade de processamento de VPN IPsec de no mínimo 14 Gbps.

Conectividade e Expansibilidade: Compatibilidade com a infraestrutura de rede atual, exigindo interfaces de 10GbE SFP+ e slots de expansão PCIe para futuras atualizações para 25G ou 100G.

Continuidade e Suporte: Adoção de metodologias de Alta Disponibilidade (HA) e suporte técnico especializado "Zero-to-Ping" para garantir a resiliência do serviço de acesso remoto.

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

a) Requisitos Internos Funcionais:

Suporte a múltiplos protocolos de VPN, especificamente IPsec, OpenVPN e WireGuard.

Capacidade de roteamento avançado baseado em políticas (Policy-based routing) e suporte a múltiplos links WAN com balanceamento de carga e failover.

Interface de gerenciamento baseada em Web (GUI) intuitiva para configuração de regras de firewall, diagnósticos e monitoramento em tempo real.

b) Requisitos Internos Não Funcionais:

Disponibilidade Física: Gabinete padrão para instalação em rack 1U com fontes de alimentação redundantes e hot-swappable para evitar interrupções por falhas elétricas.

Segurança: Atualizações de patches de segurança constantes e sem custos adicionais de licenciamento por usuário ou por túnel.

Confiabilidade: Memória com suporte a ECC (Error Correction Code) para garantir a integridade dos dados em operações críticas de rede.

c) Requisitos Externos:

Conformidade com a IN SGD/ME nº 94/2022 e alinhamento com a Estratégia de Governo Digital.

Suporte ao Programa de Gestão e Desempenho (PGD) da UFABC, viabilizando tecnicamente o regime de teletrabalho seguro para os servidores.

7. Estimativa da demanda - quantidade de bens e serviços

Tabela dos itens com quantitativos	
Descrição	Quant.
Gateway de Segurança/VPN de Alta Performance	2

Descrição da estimativa

O quantitativo de 2 (duas) unidades foi definido com base na necessidade técnica de implementar uma arquitetura de Alta Disponibilidade (High Availability - HA).

Memorial de Cálculo:

A solução de VPN da universidade é considerada um serviço crítico. Para garantir a continuidade das atividades de teletrabalho, ensino e pesquisa é indispensável a operação em regime de cluster, onde um equipamento atua como principal e o outro como contingência imediata (failover).

A estimativa de valor é da ordem de R$ 150.000,00 para o conjunto. Esse custo foi baseado em propostas de fornecedores e estudos de mercado para equipamentos de nível corporativo (Enterprise) compatíveis com as necessidades de expansão da rede institucional.

8. Levantamento de soluções

- CENÁRIO 1

- **Solução 1:** Aquisição de Appliances de Segurança e VPN de médio porte (Modelo de referência: Netgate 6100 ou equivalente).

Descrição: Equipamento de rede dedicado com processador Quad-Core (ex: Intel Atom C3558), 8GB de RAM e suporte nativo a tecnologias de aceleração de hardware como QuickAssist (QAT) e AES-NI. Possui alta densidade de portas, incluindo 10GbE SFP+, 2.5GbE e 1GbE.

Disponibilidade: Soluções baseadas em appliances de segurança com software pfSense/FreeBSD são amplamente utilizadas em órgãos da Administração Pública Federal para garantir perímetros de rede seguros e VPNs de baixo custo de licenciamento.

Alternativa de mercado: O mercado oferece appliances de diversos fabricantes (Fortinet, SonicWall, Palo Alto). No entanto, muitas dessas alternativas impõem limites artificiais de usuários ou túneis VPN e exigem licenciamento recorrente por funcionalidade, ao contrário do modelo de referência que oferece túneis e usuários ilimitados.

Solução de software: Software pfSense+ (ou equivalente de código aberto), que fornece funcionalidades completas de firewall, roteamento e VPN sem custos de licenciamento por funcionalidade.

Políticas e padrões de governo: Alinhado com os Padrões de Interoperabilidade de Governo Eletrônico (ePing), permitindo a comunicação entre diferentes sistemas governamentais, e com a Estratégia Federal de Governo Digital (Decreto 12.198/2024)

Necessidades de adequação para execução contratual: Necessita de espaço em rack (via kit de montagem opcional) ou prateleira ventilada, alimentação elétrica 12V (fonte externa inclusa) e cabos de rede compatíveis (SFP+ para 10G ou RJ-45 para 1G/2.5G)

Diferentes modelos para a prestação do serviço: Aquisição de bem permanente (hardware) com suporte técnico especializado (TAC) e atualizações de firmware inclusas

Diferentes tipos de soluções: Comparado à solução atual (Cenário 3 - servidores genéricos), o appliance de médio porte oferece refrigeração passiva (silenciosa) e menor consumo de energia, sendo ideal para unidades específicas.

Possibilidade de aquisição na forma de bens ou contratação como serviço: Aquisição como bem permanente, permitindo a incorporação ao patrimônio da universidade.

Estratégia de ampliação ou substituição da solução implantada: Visa a expansão do parque de TI para atender departamentos ou unidades com tráfego de até 1.77 Gbps em VPN IPsec.

Métricas de prestação de serviço e de pagamento: Medidas pelo throughput de VPN (Gbps), estabilidade das conexões (uptime) e tempo de resposta do suporte técnico (SLA).

Item	Investimento total - Valor(R$)				
	2026	2027	2028	2029	2030
1 (equipamentos)	R $ 12.000,00	-	-	-	-
2 (suporte)	Incluso	Incluso	Incluso	R$ 3.000,00	R$ 3.000,00
T O T A L GERAL (R$)	R $ 18.000,00				

- CENÁRIO 2

- **Solução 2:** Aquisição de Appliances de Segurança e VPN de Alta Performance (Modelo de referência: Netgate 8300 ou equivalente)

Descrição: Gateway de segurança de nível corporativo (Enterprise) em gabinete rack 1U, equipado com processador de 8 núcleos (16 threads), 32GB de RAM DDR4 ECC e armazenamento de 512GB

NVMe. A solução é otimizada para alta densidade de tráfego, oferecendo fontes de alimentação redundantes hot-swappable e suporte a aceleração de hardware Intel AVX-512.

Disponibilidade: Solução amplamente utilizada em ambientes de médio e grande porte, provedores de serviço (MSP) e instituições que exigem alta disponibilidade (HA) e grande capacidade de processamento de túneis VPN.

Alternativa de mercado: Existem alternativas de fabricantes como Fortinet ou Palo Alto; no entanto, diferentemente da solução proposta, estas geralmente impõem limites artificiais de usuários ou regras e custos recorrentes de licenciamento por funcionalidade.

Solução de software: Software pfSense+ (ou equivalente de código aberto), que oferece atualizações e patches de segurança gratuitos durante a vida útil do produto, sem taxas por usuário ou por túnel VPN.

Políticas e padrões de governo: Alinhado ao ePing (Interoperabilidade), à Estratégia Federal de Governo Digital (Decreto 12.198/2024) e ao suporte tecnológico para o Programa de Gestão e Desempenho (PGD) da UFABC.

Necessidades de adequação para execução contratual: Exige 1U de espaço em rack por equipamento, climatização de datacenter para resfriamento ativo (fluxo de ar frente-verso) e duas tomadas elétricas independentes por appliance para aproveitar a redundância das fontes.

Diferentes modelos para a prestação do serviço: Aquisição de bem permanente (hardware) com garantia de 12 meses e suporte técnico especializado "zero-to-ping" 24x7x365 incluso.

Diferentes tipos de soluções: Solução de alta performance com 11 portas independentes (1G, 2.5G e 10G) e capacidade de expansão para interfaces de 25G e 100G via slots PCIe 4.0, garantindo longevidade ao investimento.

Possibilidade de aquisição na forma de bens ou contratação como serviço: Aquisição na forma de bens (materiais), conforme registrado no DFD nº 350/2025.

Estratégia de ampliação ou substituição da solução implantada: Expansão e modernização da infraestrutura, substituindo o uso de servidores genéricos (Cenário 3) para permitir o acesso seguro de toda a comunidade universitária.

Métricas de prestação de serviço e de pagamento: Throughput de VPN IPsec de até 14.6 Gbps, estabilidade operacional via cluster de alta disponibilidade e suporte técnico especializado do fabricante.

Item	Investimento total - Valor(R$)				
	2026	2027	2028	2029	2030
1 (equipamentos)	R $ 150.000,00	-	-	-	-
2 (suporte)	Incluso	Incluso	Incluso	Incluso	incluso

TOTAL GERAL (R$)	R $ 150.000,00				

9. Análise comparativa de soluções

Sugestão para preenchimento deste tópico

Cenário	Bens / Serviços da solução	Estimativa (R$)
1	Aquisição de Appliances de Segurança e VPN de médio porte (Modelo de referência: Netgate 6100 ou equivalente)	18.000,00
2	Aquisição de Appliances de Segurança e VPN de Alta Performance (Modelo de referência: Netgate 8300 ou equivalente)	150.000,00

10. Registro de soluções consideradas inviáveis

Cenário 3: Manutenção de Servidores Genéricos (Situação Atual)

Breve Descrição: Continuidade da utilização do software pfSense instalado em hardware de servidor padrão do tipo COTS (Commercial Off-The-Shelf).

Justificativa da Inviabilidade:

Gargalo Tecnológico: O hardware genérico atual carece de aceleração específica para criptografia (como Intel QAT), o que sobrecarrega a CPU principal e reduz drasticamente a eficiência da VPN em cenários de alta carga.

Impedimento da Expansão: Esta solução foi identificada como o principal limitador que impede a expansão pretendida do serviço para toda a universidade, não resolvendo o problema de performance relatado.

Ineficiência Operacional e Econômica: Apresenta maior consumo de energia e maior ocupação de espaço em rack em comparação à appliances otimizados, além de não contar com o suporte técnico especializado "Zero-to-Ping" do fabricante, aumentando o risco de downtime prolongado.

Observação normativa: De acordo com as instruções do modelo de ETP, para as soluções registradas nesta seção, não é necessário realizar os cálculos de Custo Total de Propriedade (TCO), bastando a descrição e a justificativa técnica da inviabilidade.

Cenário 4 – Consolidação da VPN no Firewall de Borda Existente (Palo Alto PA-1410).

Breve Descrição: Utilização dos firewalls de borda atuais da instituição para a terminação de todos os túneis VPN da comunidade universitária, utilizando a tecnologia GlobalProtect.

Justificativa da Inviabilidade:

Risco de Exaustão de Recursos: O processamento massivo de criptografia (IPSec/SSL) para toda a universidade impactaria severamente o Dataplane e o Control Plane do hardware atual. Como esses equipamentos já realizam inspeção profunda de pacotes (Layer 7 e Threat Prevention), o pico de acessos VPN poderia sobrecarregar a CPU, gerando um gargalo que comprometeria não apenas o acesso remoto, mas a conectividade de internet de todos os *campi.*

Comprometimento da Segregação de Funções: A centralização de diversos serviços críticos em um único par de equipamentos cria um domínio de falha único. Em uma arquitetura desacoplada, o isolamento da VPN em hardware separado (como os appliances pretendidos no Cenário 2) garante que incidentes na VPN não afetem a segurança do núcleo da rede.

Limitações de Compatibilidade e Licenciamento: A solução apresenta dificuldades técnicas, como a ausência de um cliente nativo para sistemas Linux (comum no ambiente acadêmico) e incertezas quanto ao suporte pleno a IPv6 em túneis. Além disso, recursos avançados de segurança exigiriam licenciamento proprietário adicional em dólar, ao contrário da solução open-source do Cenário 2, que oferece usuários e túneis ilimitados sem custos extras.

Dependência de Tecnologia (Lock-in): A utilização do firewall de borda como VPN principal tornaria a instituição dependente de um único fornecedor para escalar o serviço, dificultando futuras trocas de tecnologia e gerando custos de manutenção técnica mais elevados comparados à flexibilidade do ecossistema FreeBSD /pfSense.

Em conformidade com a IN SGD/ME nº 94/2022, esta solução foi descartada por não garantir a estabilidade operacional e a escalabilidade necessárias para o suporte ao Programa de Gestão e Desempenho (PGD) da universidade.

11. Análise comparativa de custos (TCO)

1.

Cenário	Estimativa de custos (R$)				
	Ciclo de vida (em anos)	Investimento ativos	Garantia	Insumos	Manutenção
1 (Médio)	5	R$ 12.000,00	Inclusa (1 ano)	-	R$ 6.000,00
	5	R $ 150.000,00	Inclusa (1 ano)	-	-

Análise dos Custos Totais de Propriedade (Cenários)

Cenário	Solução	Valor total (R$)
1	Aquisição de Appliances de Segurança e VPN de médio porte (Modelo de referência: Netgate 6100 ou equivalente)	18.000,00
2	Aquisição de Appliances de Segurança e VPN de Alta Performance (Modelo de referência: Netgate 8300 ou equivalente)	150.000,00

Análise cenário 1: Apresenta o menor custo inicial, porém possui performance de VPN limitada a 1.77 Gbps, o que pode se tornar um novo gargalo em curto prazo com a expansão total da universidade.

Análise cenário 2: Embora exija maior investimento, oferece o melhor custo por gigabit (14.6 Gbps de VPN) e já inclui fontes redundantes, eliminando custos extras com alta disponibilidade física.

12. Descrição da solução de TIC a ser contratada

A solução escolhida é o Cenário 2, que consiste na aquisição de 2 (dois) gateways de segurança de alta performance (Nível Enterprise), com suporte a aceleração de hardware para criptografia (AVX-512) e fontes de alimentação redundantes hot-swappable.

13. Estimativa de custo total da contratação

Valor (R$): 150.000,00

Cenário nº: 2

Descrição: Aquisição de Appliances de Segurança e VPN de Alta Performance (Modelo de referência: Netgate 8300 ou equivalente)

Id	Bens / Serviços que compõem a solução	Estimativa (R$)
1	Aquisição de Appliances de Segurança e VPN de Alta Performance (Modelo de referência: Netgate 8300 ou equivalente)	150.000,00
Total		150.000,00

14. Justificativa técnica da escolha da solução

A escolha do Cenário 2 fundamenta-se na necessidade de escalabilidade. Apenas esta solução oferece processamento de até 14.6 Gbps em VPN e fontes de energia redundantes, garantindo que a expansão para toda a universidade não degrade a experiência do usuário.

15. Justificativa econômica da escolha da solução

A solução maximiza o investimento ao entregar alta performance sem taxas de licenciamento recorrente por usuário ou por túnel VPN, resultando em um menor TCO ao longo de 5 anos.

16. Benefícios a serem alcançados com a contratação

Viabilização segura do teletrabalho (PGD), eliminação de quedas por sobrecarga de hardware e garantia de acesso remoto estável para toda a comunidade acadêmica.

17. Providências a serem Adotadas

17.1. Recursos materiais necessários à implantação da solução e à continuidade do negócio

Recurso / Material 1: Espaço em rack padrão (2U no total).

Quantidade: Quatro tomadas elétricas (NEMA 5-15P ou IEC320-C15) para as fontes redundantes.

Disponibilidade: Imediata

Ação para obtenção dos recursos: Já possuímos

Responsável: NTI

17.2. Recursos humanos necessários à implantação da solução e à continuidade do negócio

Formação 1: Analistas e técnicos do NTI.

Atribuições: Configuração do cluster de alta disponibilidade, migração de regras de firewall e gerenciamento dos túneis VPN.

17.3. Estratégia de continuidade da solução em caso de interrupção contratual

Evento 1: Falha em um dos gateways de segurança.

1ª Ação Preventiva: Configuração de Cluster HA (High Availability) para failover automático entre as duas unidades

Responsável: Divisão de Redes

1ª Ação de Contingência: Manutenção temporária dos servidores genéricos atuais como cold standby durante a fase de transição.

Responsável: Divisão de Redes

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

A contratação é considerada viável, pois o investimento está alinhado ao PDTI e PCA da universidade, resolve o problema técnico de performance identificado e garante a continuidade de serviços críticos como o teletrabalho institucional (PGD) de forma econômica e escalável.

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.

CARLOS ALBERTO ORSOLON SILVA

Autoridade competente