

INST.FED.DE EDUC.,CIENC.E TEC.DO R.G.DO NORTE

Estudo Técnico Preliminar 141/2026

1. Informações Básicas

Número do processo: 23421.002414.2026-65

2. Descrição da necessidade

A presente contratação visa à aquisição de novos equipamentos de firewall de próxima geração (*Next Generation Firewall* – NGFW) para o Instituto Federal do Rio Grande do Norte – IFRN, com o objetivo de substituir equipamentos antigos atualmente em uso nos diversos campi da instituição, bem como ampliar a capacidade de proteção e disponibilidade da infraestrutura de segurança de rede da IFRN. A contratação também visa manter a padronização tecnológica já consolidada na instituição, que utiliza *firewalls* da fabricante Palo Alto Networks, bem como o software de gerenciamento centralizado Palo Alto Panorama.

O IFRN possui uma estrutura de rede distribuída entre diversos campi, cuja proteção contra ameaças cibernéticas é realizada por meio de uma solução padronizada baseada em *firewalls* de próxima geração da Palo Alto Networks e gerenciada de forma centralizada pelo software Panorama. Esta padronização foi construída ao longo de vários anos e representa um investimento significativo em ativos, capacitação técnica, integração entre sistemas e estabilidade operacional.

A solução de segurança de perímetro dos campi do IFRN é composta por equipamentos de *firewall* de próxima geração do fabricante Palo Alto Networks e gerenciados de forma centralizada através do *software* de gerenciamento Palo Alto Panorama, criando uma plataforma interoperável que consolida a segurança para a instituição. Tal cenário proporciona ganhos operacionais relevantes, como visibilidade unificada do tráfego, padronização de políticas de segurança, simplificação da gestão e maior eficiência na resposta a incidentes.

A presente contratação é motivada pela necessidade de expansão, modernização e padronização da infraestrutura de segurança de rede do Instituto Federal, considerando a criação de novos campi e a consequente ampliação do ambiente computacional institucional. O crescimento da infraestrutura de TIC impõe a adoção de mecanismos robustos de proteção, capazes de garantir a confidencialidade, integridade e disponibilidade das informações, em conformidade com as diretrizes estabelecidas pela legislação vigente, a exemplo da Lei nº 13.709/2018 (LGPD) e da Lei nº 12.965/2014 (Marco Civil da Internet).

A adoção de equipamentos do mesmo fabricante atualmente em uso permite a reaproveitamento das políticas de segurança já definidas, evita a necessidade de reconfiguração completa da infraestrutura, preserva os investimentos realizados, incluindo infraestrutura de gerenciamento centralizado, conhecimento técnico da equipe interna e processos operacionais já estabelecidos. Tal abordagem está alinhada aos princípios da economicidade, eficiência e razoabilidade previstos na Lei nº 14.133/2021, ao evitar custos desnecessários com substituição de tecnologia, retrabalho operacional e reestruturação do ambiente.

A aquisição de novos equipamentos NGFW compatíveis com a solução Palo Alto Networks, já adotada pelo IFRN, visa otimizar os investimentos realizados pela Administração. A padronização permite o aproveitamento da infraestrutura de gestão, dos processos operacionais e da capacitação técnica da equipe, evitando gastos desnecessários. A compatibilidade é essencial para garantir a interoperabilidade nativa com o ecossistema de segurança atual (Palo Alto Panorama), prevenindo a fragmentação da visibilidade de ameaças e a elevação de custos decorrentes da gestão de sistemas heterogêneos.

A presente demanda está devidamente prevista no Plano de Contratações Anual (PCA) do IFRN para o exercício de 2026 e guarda consonância com os objetivos estratégicos de segurança da informação descritos no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) vigente.

A contratação também se encontra alinhada às diretrizes da Estratégia de Governo Digital da Administração Pública Federal e às disposições da Instrução Normativa SGD/ME nº 94/2022, especialmente no que se refere ao planejamento das contratações de TIC, à segurança da informação, à continuidade dos serviços digitais e à proteção da infraestrutura tecnológica institucional.

A padronização tecnológica adotada nesta contratação encontra fundamento no art. 47, inciso I, da Lei nº 14.133 /2021, considerando a necessidade de compatibilidade técnica, interoperabilidade, integração operacional e gerenciamento unificado entre os equipamentos a serem adquiridos e a infraestrutura de segurança cibernética já implantada no IFRN, especialmente com a solução de gerenciamento centralizado Palo Alto Panorama atualmente em operação institucional.

A manutenção da arquitetura tecnológica padronizada visa assegurar a continuidade operacional dos serviços de TIC, a preservação dos investimentos públicos já realizados, a redução dos riscos de indisponibilidade e a eficiência administrativa na gestão da segurança da informação institucional.

A solução objeto desta contratação integra a arquitetura institucional de segurança cibernética do IFRN, sendo elemento crítico para proteção dos serviços digitais, integridade das informações institucionais, continuidade operacional dos ambientes acadêmicos e administrativos e atendimento às diretrizes relacionadas à segurança da informação e proteção de dados pessoais no âmbito da Administração Pública Federal.

Considerando o valor global estimado da solução e a possibilidade de limitações orçamentárias supervenientes durante o exercício, a contratação será estruturada por meio do Sistema de Registro de Preços, de modo a permitir que a Administração registre a totalidade da necessidade institucional identificada, sem que isso implique obrigação de contratação integral dos quantitativos registrados.

A adoção do Sistema de Registro de Preços permitirá ao IFRN realizar as contratações de forma gradual, conforme disponibilidade orçamentária, prioridades institucionais e cronograma de implantação definido pela área técnica, preservando a eficiência do planejamento, a continuidade da modernização da infraestrutura de segurança cibernética e a vantagem da contratação.

3. Área requisitante

Área Requisitante	Responsável
Diretoria de infraestrutura de TIC	João Rodrigo Silva de Carvalho

4. Necessidades de Negócio

1. Garantir a continuidade, a estabilidade e a segurança contra ameaças cibernéticas da infraestrutura de TI do Instituto e dos serviços providos pelo IFRN para a sociedade com o menor impacto possível na operação atual da rede;
2. Preservar os investimentos já realizados pela instituição em tecnologia, capacitação e integração de sistemas;
3. Minimizar os riscos operacionais, de indisponibilidade e de segurança relacionados a uma atualização tecnológica;
4. Assegurar gerenciamento unificado e contínuo da segurança já implementado na rede do IFRN distribuída em seus diversos campi;

5. Promover a escalabilidade e a modernização da infraestrutura de segurança da solução atual de segurança do IFRN;
6. Manter a conformidade com normas e regulamentações atendendo às exigências legais e normativas relacionadas à segurança da informação e à proteção de dados, como a Lei Geral de Proteção de Dados Pessoais (LGPD);

5. Necessidades Tecnológicas

Atualmente, a solução de segurança de rede do IFRN possui algumas das seguintes características:

- *Escalabilidade e Densidade de Usuários*: A infraestrutura de rede do IFRN atende a uma volumetria de aproximadamente 8.000 usuários simultâneos nos campi de grande porte e 600 usuários simultâneos nos campi de menor porte, o que demanda alta capacidade de gerenciamento de sessões e tabelas de estados (state tables) por parte dos ativos de segurança.
- *Monitoramento de Fluxo em Camada 7 (App-ID)*: O IFRN opera com visibilidade total de aplicações, onde todos os fluxos de dados são monitorados e classificados independentemente de porta ou protocolo, utilizando inspeção profunda de pacotes para garantir a segurança em nível de aplicação.
- *Perfil de Tráfego e Largura de Banda (Throughput)*: O ambiente possui links de internet que totalizam até 2 Gbps de banda contratada nos campi e tráfego de até 8 Gbps no Datacenter principal. O tráfego exige que o processamento de segurança (IPS, Antivírus e Threat Prevention) ocorra em velocidade de linha (wire-speed), sem gerar latência ou gargalos nos serviços acadêmicos.
- *Topologia de Rede e Resiliência (Site-to-Site VPN)*: A arquitetura de conectividade de cada campus utiliza dois links distintos: uma conexão direta ao Datacenter principal e um link de Internet. Empregamos uma VPN Site-to-Site (IPsec) estabelecida sobre o link de Internet como canal de redundância, assegurando que os serviços críticos permaneçam conectados ao Datacenter em caso de falha física do link principal.
- *Segmentação Lógica e Inspeção Inter-VLAN*: A rede interna dos campi é segmentada em até 20 VLANs. O tráfego interno (leste-oeste) é roteado e inspecionado pelos firewalls de borda, que atuam como o gateway de segurança para todas as zonas de confiança da instituição.
- *Mobilidade e Acesso Remoto (Client-to-Site VPN)*: O IFRN disponibiliza acesso remoto seguro a servidores e sistemas internos para usuários externos e administradores através de túneis SSL-VPN (Client-to-Site), exigindo a gestão centralizada de identidades e políticas de acesso criptografado.
- *Infraestrutura de Instalação e Condições Ambientais*: Os equipamentos operam instalados em racks padrão 19" em salas de ativos climatizadas, providas de sistemas de proteção elétrica (Nobreaks) e, em unidades selecionadas, suporte a grupos geradores.
- *Dinâmica de Uso e Sazonalidade*: Por ser uma instituição de ensino e pesquisa, o perfil de tráfego é intensivo em conteúdo multimídia, laboratórios virtuais e ferramentas de colaboração síncrona, apresentando picos de demanda que exigem alta disponibilidade e mecanismos de QoS para priorização de determinados tipos de tráfegos.

Outras necessidades tecnológicas necessárias à solução:

- Instalação de appliances de firewall para atender a demanda dos novos campi.
- Recursos de prevenção contra ameaças avançadas em tempo real (IPS, antivírus e proteção contra zero-day).
- Ferramentas de controle de aplicações e filtragem de conteúdo para evitar acessos a sites ou serviços indevidos.
- Alta disponibilidade, com redundância de hardware para garantir a continuidade dos serviços;
- Compatibilidade nativa com o software de gerenciamento Palo Alto Panorama atualmente utilizado pelo IFRN.

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

A solução deve possuir garantia e suporte técnico do fabricante por 60 meses para casos de problema relacionados a fabricação e receber atualizações regulares de software para resolução de bugs, correções de segurança e implantação de novos recursos/funcionalidades.

6.1. DA PARTICIPAÇÃO EM CONSÓRCIO

Considerando a natureza técnica, integrada e crítica da solução de segurança cibernética institucional pretendida, não será admitida a participação de empresas em regime de consórcio.

A solução objeto da contratação envolve elevada integração operacional entre equipamentos, licenciamento, suporte técnico especializado, gerenciamento centralizado e serviços de implantação em ambiente institucional de TIC, circunstância que exige uniformidade tecnológica, responsabilidade técnica centralizada e atuação coordenada durante toda a execução contratual.

A admissão de consórcio poderia resultar em aumento da complexidade contratual, fragmentação de responsabilidades técnicas, dificuldades de fiscalização e elevação dos riscos operacionais relacionados à interoperabilidade e continuidade da infraestrutura institucional de segurança cibernética.

Ademais, verifica-se a existência de número suficiente de empresas no mercado com capacidade técnica e operacional para execução integral do objeto, de modo que a vedação à participação em consórcio não compromete a competitividade do certame.

6.2. DA SUBCONTRATAÇÃO

Será admitida subcontratação apenas para atividades acessórias e instrumentais relacionadas à execução da solução, tais como apoio logístico, instalação física dos equipamentos ou serviços auxiliares de implantação, desde que previamente autorizada pela Administração.

Não será admitida a subcontratação integral do objeto, nem das parcelas relacionadas à responsabilidade técnica principal da solução, incluindo gerenciamento da implantação, configuração da plataforma, integração com o ambiente institucional, suporte especializado e garantia da interoperabilidade da infraestrutura de segurança cibernética.

A eventual subcontratação não afasta a responsabilidade integral da contratada perante a Administração quanto à perfeita execução do objeto contratado.

7. Estimativa da demanda - quantidade de bens e serviços

A estimativa da demanda foi elaborada com base na avaliação técnica realizada pela equipe da Diretoria de Infraestrutura de TIC (DINRE) do IFRN, levando em consideração a necessidade de substituição de *appliances* atualmente em uso, a expansão da infraestrutura de segurança perimetral para novos campi e a garantia de continuidade operacional por meio da adoção de arquitetura em alta disponibilidade.

A definição das quantidades de equipamentos e serviços considerou os critérios de obsolescência de equipamentos existentes, necessidade de cobertura de novos campi e boas práticas de gestão de TIC que preveem a existência de soluções redundantes para serviços críticos.

A contratação abrangerá tanto os equipamentos NGFW quanto os serviços de instalação, configuração e integração à solução de gerenciamento centralizado Palo Alto Panorama implantada e em uso no Instituto Federal. As quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Grupo	Id.	Descrição do Bem ou Serviço	Qtde	Métrica ou Unidade
1	1	Solução de Firewall de Próxima Geração - Tipo I (Campi) Appliance de Firewall de Próxima Geração (NGFW) de alta performance. Hardware com throughput de firewall de no mínimo 2 Gbps, capacidade de lidar com no mínimo 180.000 sessões simultâneas e 30.000 novas sessões por segundo. Inclui licenciamento de segurança avançada, garantia e suporte técnico do fabricante por 60 meses, com integração nativa a solução de firewall existente no IFRN.	27	Material
	2	Solução de Firewall de Próxima Geração - Tipo II (Datacenter) Appliance de Firewall de Próxima Geração (NGFW) de alta performance. Hardware com throughput de firewall de no mínimo 9 Gbps, capacidade de lidar com no mínimo 1.200.000 sessões simultâneas e 120.000 nova sessões por segundo. Inclui licenciamento de segurança avançada, garantia e suporte técnico do fabricante por 60 meses, com integração nativa a solução de firewall existente no IFRN.	2	Material
	3	Serviço de Instalação e Configuração da Solução de Firewall de Próxima Geração	27	Serviço
	4	Banco de Horas de 20 Horas de Serviço Técnico Especializado	5	Serviço

8. Levantamento de soluções

A equipe da Diretoria de infraestrutura de TIC do IFRN realizou um levantamento de soluções tecnológicas disponíveis no mercado que poderiam atender à demanda por modernização e ampliação da infraestrutura de segurança de rede da instituição. Foram consideradas, como premissas para essa análise, a necessidade de garantir a continuidade dos serviços críticos, a compatibilidade com a infraestrutura existente, a eficiência operacional da equipe técnica do Instituto e o alinhamento com os princípios da economicidade e da sustentabilidade do investimento público.

Alternativas tecnológicas avaliadas:

- Solução 1: Aquisição de firewalls do mesmo fabricante já utilizado pelo IFRN
- Solução 2: Aquisição de firewalls de outro fabricante

Id	Descrição da solução (ou cenário)
1	Aquisição de firewalls do mesmo fabricante já utilizado pelo IFRN Esta alternativa consiste na aquisição de novos <i>appliances</i> NGFW da mesma fabricante dos equipamentos atualmente em operação no IFRN e compatíveis com o software de gerenciamento centralizado Panorama, também já implantado e licenciado pela instituição.

2	Aquisição de firewalls de outro fabricante Esta alternativa considera a adoção de uma nova solução de segurança perimetral baseada em equipamentos de fabricante distinto ao atual. Essa aquisição implica em substituição da plataforma de gerenciamento centralizado, atualmente em uso, por uma nova, definida na arquitetura do fabricante.
---	--

A presente contratação será realizada por meio de Pregão Eletrônico para Registro de Preços, nos termos da Lei nº 14.133/2021 e do Decreto nº 11.462/2023.

A adoção do Sistema de Registro de Preços mostra-se adequada em razão da necessidade de conferir flexibilidade à Administração quanto à efetiva contratação dos quantitativos registrados, considerando que a disponibilidade orçamentária poderá variar ao longo da vigência da Ata de Registro de Preços.

Embora os quantitativos estimados representem a totalidade da necessidade institucional identificada pela área técnica, a efetiva contratação dos itens ficará condicionada à disponibilidade orçamentária do IFRN e às prioridades institucionais vigentes no momento de cada aquisição.

O critério de julgamento adotado será o de menor preço por grupo, considerando a necessidade de contratação integrada da solução tecnológica, a interoperabilidade entre os componentes, a padronização da infraestrutura institucional de segurança cibernética e a adequada definição das responsabilidades técnicas relacionadas à implantação, suporte, gerenciamento e operação da solução.

9. Análise comparativa de soluções

A seguir é apresentada a análise comparativa entre os dois cenários identificados no levantamento de soluções, considerando o atendimento as necessidades de negócio e as necessidades tecnológicas mapeadas. A análise visa identificar a alternativa mais eficaz, eficiente e efetiva para o IFRN, com base na realidade já consolidada na instituição.

A tabela abaixo consolida os requisitos avaliados e o grau de atendimento por cada solução:

Requisitos		Cenários	
		Solução 1	Solução 2
Negócio	Garantir a continuidade, a estabilidade e a segurança contra ameaças cibernéticas da infraestrutura de TI do Instituto Federal e dos serviços providos pelo IFRN para a sociedade	Atende	Atende parcialmente
	Preservar os investimentos já realizados pela instituição em tecnologia, capacitação e integração de sistemas	Atende	Não atende
	Minimizar os riscos operacionais, de indisponibilidade e de segurança relacionados a uma atualização tecnológica	Atende	Não atende
	Assegurar gerenciamento unificado e contínuo da segurança já implementado na rede do IFRN distribuída em seus diversos campi	Atende	Não atende
	Promover a escalabilidade e a modernização da infraestrutura de segurança da solução atual de segurança do IFRN	Atende	Não atende
	Manter a conformidade com normas e regulamentações atendendo às exigências legais e normativas relacionadas à segurança da informação e à proteção de dados, como a Lei Geral de Proteção de Dados Pessoais (LGPD);	Atende	Atende parcialmente
	Aquisição de appliances de firewall para atender a demanda dos novos campi	Atende	Atende

Tecnológico	Recursos de prevenção contra ameaças avançadas em tempo real (IPS, antivírus e proteção contra zero-day)	Atende	Atende
	Ferramentas de controle de aplicações e filtragem de conteúdo para evitar acessos a sites ou serviços indevidos	Atende	Atende
	Alta disponibilidade, com redundância de hardware para garantir a continuidade dos serviços	Atende	Atende
	Compatibilidade nativa com o software de gerenciamento Palo Alto Panorama atualmente utilizado pelo IFRN	Atende	Não atende
Resultado da análise		Atende	Não atende

9.1. ANÁLISE COMPARATIVA DESCRITIVA

A Solução 1 – Aquisição de firewalls do mesmo fabricante já utilizado pelo IFRN apresenta atendimento integral a todas as necessidades identificadas, tanto do ponto de vista de negócio quanto do ponto de vista técnico. Essa abordagem permite preservar a padronização tecnológica, reutilizar as políticas e configurações já definidas, garantir compatibilidade plena entre os dispositivos e evitar a necessidade de aquisição de novas ferramentas de gestão ou reconfiguração completa do ambiente.

Por sua vez, a Solução 2 – Aquisição de firewalls de outro fabricante apresenta limitações significativas em relação à continuidade operacional, compatibilidade com ferramentas já implantadas e reaproveitamento de conhecimento técnico e regras configuradas, o que compromete sua viabilidade técnica e aumenta os custos indiretos associados à migração e operação. Embora amplie a concorrência, essa abordagem demandaria a substituição completa da plataforma atual de gerenciamento, a reconfiguração de regras e políticas de segurança, a reintegração com os serviços de autenticação e rede já existentes e a capacitação da equipe técnica em novas interfaces, arquiteturas e comandos. Além disso, resultaria na descontinuidade da padronização implantada, elevando os custos operacionais e os riscos de falhas durante a transição.

10. Registro de soluções consideradas inviáveis

Como mencionado anteriormente, no processo de levantamento e análise das alternativas tecnológicas disponíveis no mercado, foram identificadas duas soluções viáveis para atender à necessidade do IFRN: Solução 1 – Aquisição de firewalls do mesmo fabricante já utilizado pelo IFRN e a Solução 2 – Aquisição de firewalls de outro fabricante.

Embora a aquisição de firewalls de outro fabricante não seja tecnicamente inviável em sentido absoluto, ela apresenta impactos operacionais e técnicos que a tornam inadequada ao contexto específico do IFRN. Dentre os principais fatores impeditivos estão a descontinuidade da ferramenta de gerenciamento centralizado Palo Alto Panorama atualmente em operação no Instituto Federal, a necessidade de reconfiguração completa das políticas de segurança, a perda de compatibilidade com os dispositivos ainda em funcionamento nos campi, o aumento da curva de aprendizado da equipe técnica e o comprometimento da estabilidade da operação durante o processo de transição tecnológica.

Dessa forma, a Solução 2 – Aquisição de firewalls de outro fabricante não se mostra viável no contexto da infraestrutura já consolidada no IFRN, sendo considerada inadequada para atender plenamente aos requisitos de negócio e as necessidades tecnológicas identificadas.

11. Análise comparativa de custos (TCO)

A tabela abaixo demonstra uma estimativa de alto nível dos custos de migração (treinamento, substituição de 100% da base instalada, horas técnicas de reconfiguração) caso houvesse substituição da plataforma tecnológica atualmente implantada:

Fator de Custo	Descrição do impacto financeiro e operacional
----------------	---

Gestão Centralizada	Necessidade de aquisição de nova licença de software de gerenciamento, visto que a licença atual do Palo Alto Panorama não possui interoperabilidade com terceiros.
Capacitação de Equipe	Custo de 80h de treinamento oficial presencial para 5 analistas da Reitoria e 25 técnicos dos campi, totalizando 2.400 horas de força de trabalho desviadas da operação para treinamento. A experiência prévia demonstra que o formato remoto é inviável para este escopo, pois a concorrência com o atendimento de demandas cotidianas prejudica o aprendizado. Portanto, a imersão presencial é necessária para garantir o aproveitamento do treinamento e o retorno do investimento
Configuração e Regras	Estimativa de 40 horas técnicas por campus para análise, tradução e conversão manual das políticas de segurança atuais para a nova sintaxe do fabricante.
Risco de Indisponibilidade	Custos intangíveis associados à potencial janela de downtime durante a migração de um ambiente crítico de rede.

11.1. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE PARA A SOLUÇÃO ADOTADA

A estimativa de custos da solução adotada concentra-se majoritariamente no primeiro ano da contratação, em virtude da aquisição dos appliances de firewall, licenças de segurança avançada, garantia e suporte técnico do fabricante com vigência de 60 (sessenta) meses.

A contratação contempla solução integrada de segurança cibernética institucional, incluindo equipamentos, licenciamento, garantia, suporte técnico especializado e serviços necessários à implantação da infraestrutura nos campi e ambientes de datacenter do IFRN.

A estratégia de contratação adotada visa assegurar estabilidade operacional, continuidade da proteção cibernética institucional e previsibilidade orçamentária ao longo do ciclo de vida da solução, mitigando riscos decorrentes de descontinuidade tecnológica, variações cambiais e elevação futura de custos de suporte e licenciamento.

Os serviços especializados de instalação, configuração, integração e suporte técnico foram incluídos na composição da solução em razão da elevada criticidade operacional da infraestrutura institucional de TIC, bem como da necessidade de implantação controlada dos appliances nos diferentes ambientes do IFRN, observando requisitos de interoperabilidade, segurança cibernética e continuidade operacional dos serviços institucionais.

A implantação da solução ocorrerá de forma planejada e gradual, conforme cronograma institucional a ser definido pela área técnica do IFRN, considerando as particularidades operacionais dos campi e dos ambientes de datacenter.

A efetiva contratação dos quantitativos registrados ocorrerá de forma gradual durante a vigência da Ata de Registro de Preços, observada a disponibilidade orçamentária da Administração e o cronograma institucional de implantação.

Solução Viável – Solução 1 – Aquisição de firewalls do mesmo fabricante já utilizado pelo IFRN						
		Anos				
Item e descrição		1	2	3	4	5
1	Solução de Firewall de Próxima Geração - Tipo I (Perfil Campi) com	R\$ 1.167.415,47	R\$	R\$	R\$	R\$ 0,00

	licenciamento e suporte técnico de 60 meses.	(27 x R\$ 43.237,61)	0,00	0,00	0,00	
2	Solução de Firewall de Próxima Geração - Tipo II (Perfil Datacenter) com licenciamento e suporte técnico de 60 meses.	R\$ 1.732.530,62 (2x R\$ 866.265,31)	R\$ 0,00	R\$ 0,00	R\$ 0,00	R\$ 0,00
3	Serviço de Instalação e Configuração da Solução de Firewall de Próxima Geração	Conforme cronograma de implantação institucional (R\$ 1.409.604,12)	R\$ 0,00	R\$ 0,00	R\$ 0,00	R\$ 0,00
4	Banco de Horas de 20 Horas de Serviço Técnico Especializado	Conforme cronograma de implantação institucional (R\$ 54.572,50)	R\$ 0,00	R\$ 0,00	R\$ 0,00	R\$ 0,00
Custo Total no Ano		R\$ 2.899.946,09	R\$ 0,00	R\$ 0,00	R\$ 0,00	R\$ 0,00
Valor depreciado (Quando aplicável)						
Custo Total de Propriedade da Solução Viável					R\$ 2.899.946,09	

Além dos custos diretos de aquisição dos appliances de segurança, a eventual substituição da plataforma atualmente implantada acarretaria custos indiretos significativos relacionados à migração tecnológica, incluindo:

- a) substituição da solução de gerenciamento centralizado Palo Alto Panorama atualmente licenciada e operacional;
- b) reconstrução integral das políticas institucionais de segurança cibernética;
- c) reprovisionamento e validação dos túneis VPN site-to-site e client-to-site;
- d) capacitação técnica especializada das equipes da Reitoria e dos campi;
- e) contratação de serviços especializados de migração e operação assistida;
- f) custos operacionais decorrentes da coexistência temporária de plataformas heterogêneas;
- g) riscos financeiros associados à indisponibilidade parcial dos serviços institucionais durante o processo de transição tecnológica.

Tais fatores demonstram que a continuidade da plataforma atualmente implantada representa a alternativa de melhor relação custo-benefício para a Administração Pública, considerando o ciclo de vida da solução e os custos totais de propriedade (TCO).

12. Descrição da solução de TIC a ser contratada

A solução de TIC a ser contratada consiste na aquisição de equipamentos de firewall de próxima geração (NGFW) da fabricante Palo Alto Networks, com desempenho compatível às necessidades de segurança, disponibilidade e expansão da infraestrutura de TIC do Instituto Federal do Rio Grande do Norte – IFRN.

A contratação abrange appliances físicos de diferentes portes, conforme as demandas específicas dos campi e data center do IFRN, além das suas respectivas licenças de segurança avançada, garantia e suporte técnico do fabricante

e serviços de instalação, configuração e integração com a ferramenta de gerenciamento centralizado Palo Alto Panorama em operação.

A escolha por dar continuidade à padronização com a fabricante Palo Alto Networks se justifica pelos seguintes diferenciais:

- Compatibilidade plena com a infraestrutura existente garantindo que todos os novos equipamentos e os equipamentos atualmente em uso no Instituto Federal serão gerenciados diretamente pelo Panorama, evitando assim que existam duas ferramentas diferentes sem qualquer integração o que dificultaria a gestão e a aplicação das políticas de segurança de uma forma unificada;
- Reaproveitamento das políticas de segurança e configurações existentes, o que reduz riscos operacionais, acelera a implantação e evita retrabalho;
- Preservação do investimento público realizado em equipamentos, licenças e capacitação da equipe técnica do IFRN ao longo dos últimos anos;
- Redução da curva de aprendizado e continuidade dos processos operacionais já consolidados, aumentando a eficiência da equipe de segurança do Instituto Federal.

12.1. MODELO DA CONTRATAÇÃO E FUNDAMENTAÇÃO LEGAL

A adoção do Sistema de Registro de Preços mostra-se adequada às características da presente contratação, uma vez que, embora os quantitativos estimados representem a totalidade da necessidade institucional identificada, não há previsão de contratação única e integral destinada ao esgotamento imediato dos quantitativos registrados.

A aquisição dos equipamentos e a contratação dos serviços ocorrerão de forma gradual, mediante contratações futuras durante a vigência da Ata de Registro de Preços, de acordo com a disponibilidade orçamentária e financeira do IFRN, as prioridades institucionais e o cronograma de implantação definido pela área técnica.

A utilização do SRP permite, assim, que a Administração registre a necessidade institucional identificada sem assumir a obrigação de contratação integral dos quantitativos, possibilitando a realização das aquisições à medida que estejam presentes as condições orçamentárias e operacionais necessárias à implantação da solução.

Dessa forma, a modelagem adotada não se destina à realização de contratação única e exauriente da Ata de Registro de Preços, mas ao atendimento gradual da demanda institucional durante sua vigência, preservando a flexibilidade administrativa, a continuidade do processo de modernização da infraestrutura de segurança cibernética e a eficiência na aplicação dos recursos públicos.

12.1.1. Justificativa para não divulgação da Intenção de Registro de Preços (IRP)

O Instituto Federal do Rio Grande do Norte – Reitoria, na condição de órgão gerenciador da Ata de Registro de Preços, será o único contratante no âmbito da presente contratação, não havendo previsão de participação de outros órgãos ou entidades.

A presente contratação será realizada por meio do Sistema de Registro de Preços, nos termos do Decreto nº 11.462 /2023.

Contudo, a divulgação da Intenção de Registro de Preços (IRP) não se mostra conveniente nem vantajosa para a Administração, uma vez que a demanda institucional já foi previamente levantada, consolidada e validada pela Diretoria de Infraestrutura de TIC do IFRN, contemplando as necessidades da Reitoria e dos campi atendidos pela infraestrutura institucional de segurança cibernética.

A governança, o planejamento e a administração da infraestrutura de segurança da informação do IFRN são realizados de forma centralizada pela Reitoria, por intermédio da área de Tecnologia da Informação e Comunicação, razão pela qual as necessidades das unidades institucionais já foram incorporadas aos quantitativos estimados da presente contratação.

Nesse contexto, a abertura de procedimento de IRP não proporcionaria ampliação relevante dos quantitativos estimados, ganho de escala ou incremento da vantajosidade da contratação, uma vez que a totalidade da demanda institucional conhecida já se encontra contemplada no planejamento realizado.

A adoção do Sistema de Registro de Preços decorre exclusivamente da necessidade de conferir flexibilidade à Administração quanto ao momento e ao quantitativo efetivamente contratado, considerando a possibilidade de restrições ou contingenciamentos orçamentários durante a vigência da Ata de Registro de Preços. Assim, embora os quantitativos registrados representem a necessidade institucional integral identificada pela área técnica, a efetiva contratação dos itens permanecerá condicionada à disponibilidade orçamentária e financeira do IFRN.

Adicionalmente, a realização da IRP acarretaria ampliação do prazo de tramitação do procedimento licitatório, sem geração de benefícios concretos para a Administração, retardando a disponibilização da solução necessária à modernização da infraestrutura institucional de segurança cibernética e à continuidade dos serviços digitais do IFRN.

Dessa forma, considerando a consolidação prévia da demanda institucional, a inexistência de ganhos decorrentes da participação de outros órgãos e a necessidade de conferir maior celeridade à contratação, justifica-se a não divulgação da Intenção de Registro de Preços (IRP), nos termos da legislação vigente.

13. Estimativa de custo total da contratação

Valor (R\$): 4.364.122,70

O valor global estimado para o atendimento pleno das necessidades do Instituto Federal do Rio Grande do Norte (IFRN) é de R\$ 4.364.122,70, conforme detalhado na tabela subsequente.

Item	Descrição	Quantidade	Valor Unitário Cotado	Valor Total
1	Solução de Firewall de Próxima Geração - Tipo I (campi)	27	R\$ 43.237,61	R\$ 1.167.415,47
2	Solução de Firewall de Próxima Geração - Tipo II (datacenter)	2	R\$ 866.265,31	R\$ 1.732.530,62
3	Serviço de Instalação e Configuração da Solução de Firewall de Próxima Geração	29	R\$ 52.207,56	R\$ 1.409.604,12
4	Banco de Horas de 20 Horas de Serviço Técnico Especializado	5	R\$ 10.914,50	R\$ 54.572,50
Total				R\$ 4.364.122,71

A estimativa do custo total desta contratação foi realizada em estrita observância ao disposto no art. 23 da Lei nº 14.133/2021 e nas normativas vigentes da SGD/MGI, baseando-se em ampla pesquisa de mercado que buscou refletir os preços praticados na Administração Pública e pelos fornecedores de firewalls no Brasil. Para a definição do valor estimado, foram utilizados os parâmetros dos incisos I (pesquisa de preços do portal de compras governamentais) e IV (cotação direta com fornecedores) do art. 5º da Instrução Normativa SEGES/ME nº 65/2021.

A estimativa do custo total desta contratação foi realizada em observância ao disposto no art. 23 da Lei nº 14.133/2021 e às normativas aplicáveis às contratações de Tecnologia da Informação e Comunicação no âmbito da Administração Pública Federal, baseando-se em ampla pesquisa de mercado voltada à identificação dos preços praticados pela Administração Pública e por fornecedores especializados no segmento de segurança cibernética.

Para definição do valor estimado foram utilizados os parâmetros previstos nos incisos I e IV do art. 5º da Instrução Normativa SEGES/ME nº 65/2021, considerando pesquisa em contratações públicas similares e cotações diretas junto a fornecedores especializados.

O valor global estimado contempla a solução completa de modernização da infraestrutura de segurança cibernética institucional do IFRN, incluindo appliances NGFW, licenciamento, garantia, suporte técnico especializado e serviços necessários à implantação e integração da solução nos ambientes institucionais.

14. Justificativa técnica da escolha da solução

A escolha pela contratação de equipamentos de firewall de próxima geração da fabricante Palo Alto Networks decorre da necessidade institucional de manutenção da padronização tecnológica da infraestrutura de segurança cibernética do IFRN, atualmente estruturada sobre arquitetura integrada composta por appliances NGFW e pela solução de gerenciamento centralizado Palo Alto Panorama já implantada e operacional na instituição.

A restrição à referida plataforma não decorre de preferência subjetiva por marca, mas da necessidade técnica de assegurar compatibilidade integral, interoperabilidade nativa, continuidade operacional, gerenciamento centralizado, reaproveitamento das políticas de segurança já configuradas e preservação dos investimentos públicos anteriormente realizados em equipamentos, licenças, capacitação da equipe técnica e processos operacionais.

A adoção de equipamentos de fabricante diverso implicaria a coexistência de plataformas heterogêneas, fragmentação da gestão da segurança institucional, necessidade de utilização de consoles distintos, reconfiguração integral das políticas de segurança, reintegração com serviços de autenticação e rede, aumento da curva de aprendizado da equipe técnica, maior risco de falhas operacionais e potencial comprometimento da disponibilidade dos serviços digitais prestados pelo IFRN.

Assim, a padronização na plataforma Palo Alto Networks encontra respaldo no art. 47, inciso I, da Lei nº 14.133/2021, considerando a necessidade de compatibilidade técnica, integração operacional, economicidade, eficiência administrativa, continuidade dos serviços públicos digitais e preservação da segurança da informação institucional.

14.1. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENDE DE ASPECTOS TÉCNICOS

O parcelamento da contratação da solução não se mostra tecnicamente viável, visto tratar-se de uma plataforma integrada cujos componentes são interdependentes para garantir a eficácia e a resiliência necessárias para proteção contra ataques cibernéticos. O agrupamento dos itens que compõem esta solução representa a melhor estratégia para a Administração Pública, em consonância com as boas práticas de governança e gestão de Tecnologia da Informação, que preveem a adoção de plataformas integradas para garantir segurança, eficiência operacional e facilidade na gestão do ambiente de TIC.

A divisão deste objeto em múltiplos contratos ou fornecedores implicaria em graves riscos à operacionalização e à efetividade da solução, sendo inviável a sua fragmentação, pelos seguintes motivos:

- a) Implicaria em sobrecarga da área administrativa, que teria que gerenciar múltiplos contratos e fornecedores para componentes interdependentes;
- b) Aumentaria a complexidade do controle e fiscalização do contrato, exigindo maior esforço para garantir o cumprimento de requisitos técnicos e a integração entre diferentes prestadores;
- c) Geraria sobreposição de atividades e riscos de falhas de responsabilidade entre fornecedores, o que comprometeria a segurança e a continuidade dos serviços;

A contratação sob um único grupo viabiliza maior eficiência no gerenciamento do objeto contratado, promove a unificação das atividades de suporte e atualização da solução, reduz a possibilidade de lacunas na integração entre funcionalidades críticas e assegura o atingimento dos objetivos institucionais de segurança da informação e proteção de dados sensíveis.

Dessa forma, a fragmentação do objeto não apenas comprometeria a execução integrada e eficiente da solução, como também não resultaria em melhor aproveitamento do mercado, tampouco ampliaria a competitividade do certame. Pelo contrário, elevaria o risco de falhas operacionais e de segurança.

O não parcelamento da solução encontra fundamento no art. 40, §3º, e no art. 47, inciso II, da Lei nº 14.133/2021, considerando que a fragmentação do objeto comprometeria a integração operacional da solução, a uniformidade tecnológica da infraestrutura de segurança institucional e a adequada definição das responsabilidades técnicas relacionadas ao suporte, interoperabilidade, atualização e gerenciamento centralizado da plataforma.

14.2. JUSTIFICATIVA DA PADRONIZAÇÃO TECNOLÓGICA

O IFRN possui atualmente uma arquitetura institucional de segurança cibernética padronizada baseada em equipamentos de firewall de próxima geração (NGFW) da fabricante Palo Alto Networks, integrados à solução de gerenciamento centralizado Palo Alto Panorama, implantada e operacional em diversos campi da instituição.

A referida infraestrutura foi construída ao longo de vários anos, envolvendo investimentos públicos relevantes em aquisição de ativos, licenciamento, integração tecnológica, definição de políticas institucionais de segurança, capacitação técnica das equipes da Reitoria e dos campi, bem como consolidação de processos operacionais relacionados à gestão da segurança da informação institucional.

A manutenção da padronização tecnológica apresenta-se como medida necessária para assegurar:

- a) interoperabilidade nativa entre os equipamentos atualmente em operação e os novos appliances a serem adquiridos;
- b) gerenciamento centralizado e unificado da segurança cibernética institucional;
- c) reaproveitamento integral das políticas de segurança, regras, objetos, perfis, logs e túneis VPN já configurados no ambiente institucional;
- d) continuidade operacional da infraestrutura de TIC do IFRN;
- e) preservação dos investimentos públicos anteriormente realizados;
- f) redução de riscos operacionais e de indisponibilidade decorrentes de processos de migração tecnológica.

A adoção de solução tecnológica diversa implicaria a coexistência de plataformas heterogêneas de segurança, resultando em fragmentação operacional, utilização de múltiplos consoles de gerenciamento, aumento da complexidade administrativa, elevação da superfície de risco cibernético e necessidade de reconstrução integral da arquitetura de segurança atualmente implantada.

Assim, a padronização tecnológica adotada nesta contratação encontra fundamento no art. 47, inciso I, da Lei nº 14.133/2021, considerando a necessidade de compatibilidade técnica, integração operacional, economicidade, eficiência administrativa, continuidade dos serviços públicos digitais e preservação da segurança cibernética institucional.

14.3. RISCOS DA DESCONTINUIDADE DA PLATAFORMA TECNOLÓGICA

A substituição da plataforma de segurança atualmente implantada no IFRN ou a adoção de solução tecnológica heterogênea acarretaria riscos operacionais significativos à infraestrutura institucional de TIC.

Dentre os principais riscos identificados destacam-se:

- a) perda da gestão centralizada da segurança institucional atualmente realizada por meio do Palo Alto Panorama;
- b) fragmentação das políticas de segurança e perda de visibilidade unificada dos eventos de rede e incidentes cibernéticos;
- c) aumento da complexidade operacional da equipe técnica responsável pela administração da infraestrutura de segurança;
- d) necessidade de reconfiguração integral das regras, objetos, políticas, túneis VPN e mecanismos de autenticação atualmente implantados;
- e) aumento do tempo de resposta a incidentes de segurança;
- f) elevação do risco de indisponibilidade dos serviços digitais institucionais durante eventual processo de migração tecnológica;
- g) aumento da superfície de risco cibernético decorrente da coexistência de plataformas distintas sem interoperabilidade nativa;
- h) necessidade de investimentos adicionais em capacitação técnica, consultoria especializada e substituição da infraestrutura de gerenciamento centralizado.

Dessa forma, a manutenção da plataforma tecnológica atualmente utilizada mostra-se necessária para assegurar a continuidade operacional dos serviços institucionais e a estabilidade da arquitetura de segurança cibernética do IFRN.

15. Justificativa econômica da escolha da solução

A escolha pela continuidade da solução de segurança baseada em equipamentos da fabricante Palo Alto Networks apresenta-se como a alternativa mais econômica para o Instituto Federal do Rio Grande do Norte – IFRN, considerando não apenas o custo direto de aquisição, mas, principalmente, os custos indiretos relacionados à implantação, operação, manutenção e capacitação técnica.

A padronização tecnológica já consolidada na instituição com a plataforma Palo Alto permite a continuidade da estrutura de gerenciamento centralizado através da ferramenta Palo Alto Panorama, cujas licenças e suporte encontram-se ativos, evitando a necessidade de aquisição de uma nova ferramenta de administração centralizada.

Além disso, a equipe técnica do IFRN, tanto na Reitoria quanto nos campi, já se encontra plenamente capacitada para operar a solução atualmente utilizada, o que afasta a necessidade de investimentos adicionais em treinamentos, certificações ou suporte técnico especializado — custos que seriam inevitáveis na adoção de uma nova tecnologia. Essa familiaridade operacional também contribui para reduzir o tempo de implantação e de resolução de eventuais falhas, mitigando riscos de indisponibilidade e minimizando impactos na continuidade dos serviços prestados pelo Instituto Federal à sociedade.

Outro fator de economia é o reaproveitamento de políticas de segurança e regras já definidas, evitando a alocação de recursos para reconstrução de toda a arquitetura de segurança institucional. A continuidade da plataforma reduz

também os custos com suporte de terceiros, já que a integração entre dispositivos novos e antigos se dá de forma nativa.

Portanto, a continuidade com a fabricante Palo Alto Networks representa a alternativa mais racional e economicamente vantajosa, ao evitar desperdícios, retrabalhos e gastos desnecessários com adaptações tecnológicas ou operacionais.

15.2. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS

O agrupamento dos itens em grupo único também contribui para uniformização da responsabilidade técnica da solução, mitigação de riscos operacionais, simplificação da gestão contratual e garantia de interoperabilidade entre os componentes críticos da infraestrutura de segurança cibernética institucional.

O não parcelamento da solução encontra fundamento no art. 40, §3º, e no art. 47, inciso II, da Lei nº 14.133/2021, considerando que a fragmentação do objeto comprometeria a integração operacional da solução, a uniformidade tecnológica da infraestrutura institucional e a adequada definição das responsabilidades relacionadas à implantação, suporte, atualização e gerenciamento centralizado da plataforma.

16. ATENDIMENTO À LISTA DE VERIFICAÇÃO - AGU

A presente contratação foi estruturada em observância às orientações constantes nos instrumentos de padronização e listas de verificação elaboradas pela Advocacia-Geral da União aplicáveis às contratações de Tecnologia da Informação e Comunicação.

A solução proposta encontra-se devidamente alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) vigente e ao Plano de Contratações Anual (PCA) do IFRN, em conformidade com as disposições da Instrução Normativa SGD/ME nº 94/2022.

A padronização tecnológica adotada nesta contratação encontra fundamento no art. 47, inciso I, da Lei nº 14.133/2021, considerando a necessidade de compatibilidade técnica, interoperabilidade, continuidade operacional, gerenciamento centralizado da segurança institucional e preservação dos investimentos públicos já realizados pelo IFRN.

O agrupamento dos itens em grupo único e o não parcelamento da solução encontram respaldo no art. 40, §3º, e no art. 47, inciso II, da Lei nº 14.133/2021, considerando a natureza integrada da solução de segurança cibernética institucional e a necessidade de uniformidade tecnológica da infraestrutura de TIC.

A estimativa de preços foi realizada em observância ao art. 23 da Lei nº 14.133/2021 e à Instrução Normativa SEGES/ME nº 65/2021, mediante utilização de pesquisa em contratações públicas similares e cotações junto a fornecedores especializados.

A contratação observará ainda os princípios da eficiência, economicidade, continuidade dos serviços públicos digitais, segurança da informação e proteção de dados pessoais, em consonância com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e com as diretrizes de segurança cibernética aplicáveis à Administração Pública Federal.

O valor da contratação atrai a incidência da IN 94/2022?

A presente contratação atrai integralmente a incidência da Instrução Normativa SGD/ME nº 94/2022, considerando que o valor estimado da contratação é superior ao limite previsto no art. 75, inciso II, da Lei nº 14.133/2021 para contratações diretas por dispensa em razão do valor.

Trata-se de contratação de solução estratégica de Tecnologia da Informação e Comunicação (TIC), envolvendo aquisição de equipamentos de firewall de próxima geração (NGFW), licenciamento, suporte técnico especializado e serviços de implantação e integração da infraestrutura institucional de segurança cibernética do IFRN, circunstância

que enquadra integralmente a demanda no escopo de aplicação da IN SGD/ME nº 94/2022, nos termos do art. 1º da referida norma.

Dessa forma, o planejamento da contratação observou as diretrizes aplicáveis às contratações de TIC no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, especialmente quanto ao alinhamento ao PDTIC institucional, à justificativa técnica da solução, à padronização tecnológica, à gestão de riscos e à definição dos requisitos técnicos e operacionais da contratação.

Caso o valor estimado da contratação atraia a necessidade de sua aprovação pelo Órgão Central do SISP, ela foi obtida?

Não. Embora a presente contratação esteja submetida às disposições da IN SGD/ME nº 94/2022, ela não se enquadra nas hipóteses que demandam submissão prévia à aprovação do Órgão Central do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, tratando-se de contratação institucional específica do IFRN destinada à modernização da infraestrutura local de segurança cibernética.

A Administração registrou que o objeto da contratação NÃO incide nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD nº 94/2022?

A presente contratação não incide nas hipóteses vedadas pelos arts. 3º e 4º da Instrução Normativa SGD/ME nº 94 /2022.

A solução objeto desta contratação refere-se à aquisição de equipamentos de firewall de próxima geração (NGFW), licenciamento, suporte técnico especializado e serviços acessórios de implantação e integração, não abrangendo atividades de gestão de processos de Tecnologia da Informação, gestão de segurança da informação institucional, desenvolvimento estratégico de software ou transferência indevida de competências típicas da Administração Pública.

Os serviços previstos possuem natureza eminentemente técnica e acessória, limitando-se à instalação, configuração, integração, suporte e operação assistida da solução contratada, sem caracterização de vínculo de subordinação, alocação de mão de obra típica de atividade finalística da Administração ou transferência de responsabilidade decisória relacionada à governança de TIC do IFRN.

A gestão da infraestrutura institucional de segurança cibernética, a definição das políticas de segurança da informação, a administração dos ambientes institucionais e a tomada de decisões estratégicas permanecerão integralmente sob responsabilidade do IFRN.

A Administração registrou ter observado os guias, manuais e modelos publicados pelo Órgão Central do SISP?

A presente contratação observou, no que aplicável, os guias, manuais, orientações técnicas, modelos e instrumentos de padronização publicados pelo Órgão Central do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, especialmente aqueles relacionados ao planejamento das contratações de Tecnologia da Informação e Comunicação, à gestão de riscos, à segurança da informação e à elaboração dos artefatos de planejamento previstos na Instrução Normativa SGD/ME nº 94/2022.

Foram igualmente observadas as orientações constantes nos modelos e listas de verificação disponibilizados pela Advocacia-Geral da União aplicáveis às contratações de TIC no âmbito da Administração Pública Federal.

Caso a solução escolhida, resultante do Estudo Técnico Preliminar, contenha item presente nos Catálogos de Soluções de TIC com Condições Padronizadas publicados pelo Órgão Central do SISP no âmbito do processo de gestão estratégica das contratações de soluções baseadas em software de uso disseminado previsto no § 2º do art. 43 da Lei nº 14.133, de 2022, os documentos de planejamento da contratação utilizaram todos os elementos constantes no respectivo Catálogo, tais como: especificações técnicas, níveis de serviços, códigos de catalogação, PMC-TIC, entre outros?

Não foram identificados, até o momento da elaboração dos artefatos de planejamento da contratação, Catálogos de Soluções de TIC com Condições Padronizadas publicados pelo Órgão Central do SISP aplicáveis de forma integral à presente solução de segurança cibernética institucional.

A solução objeto da contratação possui características técnicas especializadas relacionadas à infraestrutura institucional de firewall de próxima geração (NGFW), interoperabilidade com plataforma de gerenciamento centralizado Palo Alto Panorama e requisitos específicos de segurança cibernética do IFRN, não se enquadrando nas hipóteses típicas de soluções padronizadas de software de uso disseminado previstas no §2º do art. 43 da Lei nº 14.133/2021.

Não obstante, foram observadas, no que aplicável, as diretrizes gerais, boas práticas e orientações técnicas publicadas pelo Órgão Central do SISP aplicáveis às contratações de TIC.

Foi certificado que objeto da contratação está compatível com as leis orçamentárias?

Sim. A presente contratação encontra-se compatível com as leis orçamentárias vigentes, em especial com a Lei Orçamentária Anual (LOA), o Plano Plurianual (PPA) e a Lei de Diretrizes Orçamentárias (LDO), observando as disposições do art. 18 da Lei nº 14.133/2021.

A demanda encontra-se prevista no Plano de Contratações Anual (PCA) do IFRN para o exercício de 2026, bem como alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) institucional, estando compatível com o planejamento estratégico e orçamentário da instituição.

A contratação visa assegurar a continuidade operacional da infraestrutura institucional de segurança cibernética, a proteção dos serviços digitais e a modernização da infraestrutura de TIC do IFRN, em consonância com os objetivos institucionais e as diretrizes de governança pública aplicáveis.

Foi elaborado o Estudo Técnico Preliminar da Contratação, exigido pelo art. 9º, II, e art. 11 da IN SGD nº 94/2022?

Sim. A presente contratação foi precedida da elaboração do Estudo Técnico Preliminar (ETP), em observância ao disposto nos arts. 9º, inciso II, e 11 da Instrução Normativa SGD/ME nº 94/2022.

O ETP contemplou a identificação da necessidade institucional, o levantamento e análise das alternativas tecnológicas disponíveis no mercado, a definição dos requisitos técnicos e operacionais da solução, a análise comparativa das alternativas avaliadas, a justificativa da solução escolhida, a estimativa de custos, a avaliação dos benefícios esperados e a demonstração da viabilidade técnica e econômica da contratação.

O documento também observou as diretrizes de planejamento das contratações de TIC aplicáveis à Administração Pública Federal, incluindo aspectos relacionados à padronização tecnológica, segurança cibernética, interoperabilidade, continuidade operacional e alinhamento ao PDTIC institucional.

O Estudo Técnico Preliminar contempla todos os elementos compreendidos no art. 11 da IN SGD nº 94/2022?

Sim. O Estudo Técnico Preliminar elaborado para a presente contratação contempla os elementos exigidos pelo art. 11 da Instrução Normativa SGD/ME nº 94/2022, observando as diretrizes aplicáveis ao planejamento das contratações de soluções de Tecnologia da Informação e Comunicação no âmbito da Administração Pública Federal.

Foi consultado o Guia Nacional de Contratações Sustentáveis da Consultoria Geral da União para inserção dos critérios de sustentabilidade?

Sim. Para elaboração dos artefatos de planejamento da presente contratação foram observadas, no que aplicável, as orientações constantes no Guia Nacional de Contratações Sustentáveis da Consultoria-Geral da União, especialmente quanto à avaliação de critérios de sustentabilidade aplicáveis às contratações de Tecnologia da Informação e Comunicação.

Considerando as características da solução pretendida, foram incorporadas medidas relacionadas à eficiência energética dos equipamentos, ampliação da vida útil dos ativos de TIC, racionalização da infraestrutura tecnológica institucional e descarte ambientalmente adequado dos equipamentos substituídos.

Registra-se ainda que a natureza técnica e especializada da solução de segurança cibernética limita parcialmente a aplicação de determinados critérios sustentáveis padronizados, razão pela qual foram adotadas as medidas compatíveis com as especificidades operacionais e tecnológicas da contratação.

A justificativa para a contratação contemplou as exigências do artigo 15 da IN SGD nº 94/2022 e, em caso de compras, também do art. 12, § 7º, da mesma IN?

Sim. A justificativa da presente contratação contemplou os elementos exigidos pelo art. 15 da Instrução Normativa SGD/ME nº 94/2022, bem como, no que aplicável à aquisição de bens de TIC, as disposições do art. 12, §7º, da referida norma.

A documentação de planejamento da contratação apresentou:

- a motivação da contratação;
- a demonstração da necessidade institucional;
- a justificativa técnica da solução escolhida;
- a análise de padronização tecnológica;
- os requisitos técnicos e operacionais da solução;
- a estimativa de demanda;
- a análise comparativa entre alternativas tecnológicas;
- a justificativa do agrupamento e do não parcelamento;
- a estimativa de custos;
- os benefícios esperados;
- os requisitos de garantia, suporte técnico e interoperabilidade;
- o alinhamento ao PDTIC institucional e ao planejamento estratégico do IFRN.

Adicionalmente, considerando tratar-se de aquisição de solução de TIC composta por equipamentos de firewall de próxima geração (NGFW), foram observados aspectos relacionados às especificações técnicas da solução, requisitos de desempenho, integração à infraestrutura institucional existente, garantia, suporte técnico especializado e condições necessárias à implantação e operação segura da solução no ambiente institucional do IFRN.

Tratando-se de licitação para fornecimento de bens, em caso de indicação de uma ou mais marcas ou modelos, o que se admite apenas excepcionalmente, foi apresentado o estudo técnico, fundamentado nas alíneas do art. 41, I, da Lei nº 14.133/2021, que justifique essa opção?

Sim. Considerando que a solução pretendida contempla a padronização tecnológica da infraestrutura institucional de segurança cibernética baseada na plataforma Palo Alto Networks, foi elaborado estudo técnico contendo a fundamentação necessária para justificar a indicação da fabricante, em observância ao art. 41, inciso I, da Lei nº 14.133/2021.

A justificativa encontra-se baseada, especialmente, nas seguintes hipóteses previstas no referido dispositivo legal:

- necessidade de padronização da infraestrutura tecnológica institucional;
- compatibilidade técnica e interoperabilidade com a solução de gerenciamento centralizado Palo Alto Panorama já implantada e operacional no IFRN;

- preservação dos investimentos públicos anteriormente realizados em equipamentos, licenciamento, capacitação técnica e processos operacionais;
- necessidade de continuidade operacional da infraestrutura de segurança cibernética institucional;
- mitigação de riscos operacionais decorrentes da coexistência de plataformas heterogêneas de segurança;
- garantia de gerenciamento centralizado, uniformidade das políticas de segurança e integração nativa entre os componentes da solução.

O Estudo Técnico Preliminar também demonstrou que a adoção de solução tecnológica diversa implicaria elevados impactos operacionais, financeiros e de segurança cibernética, incluindo necessidade de substituição da infraestrutura de gerenciamento existente, reconstrução integral das políticas institucionais de segurança e aumento da complexidade operacional da infraestrutura institucional de TIC do IFRN.

Caso o objeto contratual diga respeito a algum dos itens abaixo, foi atestado nos autos o cumprimento do Anexo I da IN SGD nº 94/2022?

- Licenciamento de software e serviços agregados;
- Solução de autenticação para serviços públicos digitais;
- Serviços de desenvolvimento, sustentação e manutenção de software;
- Infraestrutura de centro de dados, serviços em nuvem, sala-cofre ou sala segura;
- Contratação de empresas públicas de tecnologia da informação e comunicação;
- Serviços de desenvolvimento, sustentação e manutenção de portais na internet;
- Aquisições de ativos de tecnologia da Informação e Comunicação.

Sim. A presente contratação enquadra-se na hipótese de aquisição de ativos de Tecnologia da Informação e Comunicação, abrangendo equipamentos de firewall de próxima geração (NGFW), licenciamento, suporte técnico especializado e serviços acessórios de implantação e integração.

Nesse contexto, registra-se que os artefatos de planejamento da contratação observaram, no que aplicável, as disposições constantes do Anexo I da Instrução Normativa SGD/ME nº 94/2022, especialmente quanto:

- à definição dos requisitos técnicos e operacionais da solução;
- às especificações técnicas dos ativos de TIC;
- à padronização tecnológica institucional;
- aos requisitos de garantia e suporte técnico;
- aos critérios de interoperabilidade e integração;
- aos requisitos de segurança da informação e continuidade operacional;
- à estimativa de custos e análise de viabilidade da contratação.

Considerando as características específicas da solução de segurança cibernética institucional pretendida, foram observados os elementos aplicáveis às aquisições de ativos de TIC compatíveis com a natureza técnica e operacional da contratação.

Em caso de licitação por preço global, foi observado que cada serviço ou produto do lote deve estar discriminado em itens separados nas propostas de preços, permitindo a identificação do preço individual e a eventual incidência das margens de preferência?

Sim. Embora a contratação adote critério de julgamento por grupo, os itens que compõem a solução encontram-se individualmente discriminados no Estudo Técnico Preliminar e serão igualmente detalhados no Termo de Referência e no modelo de proposta comercial, com identificação dos respectivos quantitativos e valores unitários, em observância aos princípios da transparência, competitividade e julgamento objetivo.

A modelagem adotada permitirá a identificação individualizada dos preços dos equipamentos, licenças, serviços especializados e demais componentes da solução, possibilitando a adequada análise da formação dos preços, da vantajosidade da proposta e da eventual incidência de margens de preferência legalmente aplicáveis, sem prejuízo da contratação integrada da solução tecnológica em grupo único.

A especificação dos requisitos da contratação foi realizada conforme o art. 16, I e II, e parágrafo único, da IN SGD nº 94, de 2022?

Sim. A especificação dos requisitos da contratação foi elaborada em conformidade com o art. 16, incisos I e II, e parágrafo único, da Instrução Normativa SGD/ME nº 94/2022, contemplando os requisitos de negócio e os requisitos tecnológicos necessários à adequada definição da solução de TIC pretendida.

O Estudo Técnico Preliminar apresentou de forma estruturada:

- as necessidades de negócio relacionadas à continuidade operacional da infraestrutura institucional de segurança cibernética;
- os requisitos tecnológicos associados à interoperabilidade, gerenciamento centralizado, desempenho, disponibilidade, escalabilidade e segurança da solução;
- os requisitos de compatibilidade com a infraestrutura atualmente implantada no IFRN;
- os requisitos de garantia, suporte técnico e atualização tecnológica;
- os requisitos relacionados à proteção da informação, disponibilidade dos serviços digitais e continuidade operacional da infraestrutura institucional de TIC.

Adicionalmente, foram considerados aspectos relacionados à padronização tecnológica institucional, integração nativa com a solução Palo Alto Panorama, mitigação de riscos operacionais e atendimento às necessidades específicas da arquitetura de segurança cibernética do IFRN, em observância às diretrizes da IN SGD/ME nº 94/2022.

As responsabilidades da contratante, contratada e órgão gerenciador (quando aplicáveis) foram definidas em conformidade com os requisitos do artigo 17 da IN SGD nº 94/2022?

Sim. As responsabilidades da contratante e da contratada serão definidas no Termo de Referência da contratação, em conformidade com o art. 17 da Instrução Normativa SGD/ME nº 94/2022, contemplando os aspectos relacionados à implantação, suporte técnico, garantia, gestão da solução, fiscalização contratual, segurança da informação e continuidade operacional da infraestrutura institucional de TIC.

Considerando que a presente contratação adotará Sistema de Registro de Preços, a Reitoria do IFRN atuará como órgão gerenciador da Ata de Registro de Preços, sendo responsável pelo gerenciamento, controle dos quantitativos registrados e demais atribuições previstas no Decreto nº 11.462/2023.

Caso o objeto contemple itens com valores inferiores a R\$80.000,00, eles foram destinados às ME/EPPs e entidades equiparadas ou foi justificada a não exclusividade?

Embora a contratação contemple item com valor estimado inferior a R\$ 80.000,00, não foi adotada exclusividade para participação de microempresas e empresas de pequeno porte, em razão da necessidade de contratação integrada da solução de segurança cibernética institucional.

A solução pretendida possui elevada integração técnica e operacional entre equipamentos, licenciamento, suporte técnico especializado e serviços acessórios de implantação e sustentação, circunstância que inviabiliza o fracionamento do objeto sem comprometimento da interoperabilidade, da padronização tecnológica e da adequada execução contratual.

A segregação de itens isolados comprometeria a uniformidade da solução, dificultaria a definição de responsabilidades técnicas, aumentaria os riscos operacionais relacionados à segurança cibernética institucional e poderia resultar em incompatibilidades técnicas entre os componentes da infraestrutura.

Dessa forma, a não adoção da exclusividade prevista nos arts. 47 e 48 da Lei Complementar nº 123/2006 encontra-se justificada em razão da inviabilidade técnica do parcelamento e da necessidade de preservação da integração operacional da solução contratada.

Caso tenha sido vedada a participação de cooperativas, consta justificativa nos autos?

Considerando as características técnicas e operacionais da presente contratação, não será admitida a participação de cooperativas.

A solução objeto da contratação envolve fornecimento integrado de equipamentos especializados de segurança cibernética, licenciamento, suporte técnico do fabricante, implantação, integração e serviços técnicos especializados de elevada complexidade operacional, demandando estrutura empresarial compatível, responsabilidade técnica centralizada e capacidade de coordenação contínua da execução contratual.

A natureza do objeto exige atuação empresarial organizada, integração operacional entre os componentes da solução e responsabilidade técnica unificada quanto à interoperabilidade, suporte especializado, garantia da solução e continuidade operacional da infraestrutura institucional de TIC do IFRN.

Dessa forma, a vedação à participação de cooperativas decorre das especificidades técnicas da contratação e da necessidade de assegurar a adequada execução da solução de segurança cibernética institucional, sem prejuízo à competitividade do certame.

Caso tenha sido vedada a participação de consórcios, consta justificativa nos autos?

Sim. A vedação à participação de empresas em regime de consórcio encontra-se devidamente justificada nos autos, considerando as características técnicas, operacionais e de segurança cibernética da solução pretendida.

A contratação envolve solução integrada de firewall de próxima geração (NGFW), composta por equipamentos, licenciamento, suporte técnico especializado, gerenciamento centralizado e serviços críticos de implantação e integração à infraestrutura institucional de TIC do IFRN. Tal contexto exige uniformidade tecnológica, responsabilidade técnica centralizada, interoperabilidade plena entre os componentes da solução e atuação coordenada durante toda a execução contratual.

A admissão de consórcios poderia resultar em fragmentação de responsabilidades técnicas, aumento da complexidade da gestão contratual, dificuldades de fiscalização e elevação dos riscos operacionais relacionados à continuidade da infraestrutura institucional de segurança cibernética.

Além disso, verificou-se a existência de número suficiente de empresas no mercado com capacidade técnica e operacional para execução integral do objeto, de modo que a vedação à participação em consórcio não compromete a competitividade do certame.

Consta dos autos a motivação sobre o momento da divulgação do orçamento da licitação?

O orçamento estimado da contratação será divulgado juntamente com os demais documentos do certame, em observância aos princípios da transparência e publicidade, considerando que a ampla divulgação dos valores estimados não compromete a competitividade da contratação.

Foi certificado que a aquisição e o pagamento observarão condições semelhantes às do setor privado ou houve justificativa para não observância dessas condições?

Sim. A presente contratação foi estruturada observando práticas usuais do mercado de soluções corporativas de Tecnologia da Informação e Comunicação, especialmente no segmento de segurança cibernética e infraestrutura de firewall de próxima geração (NGFW).

As condições relacionadas ao fornecimento dos equipamentos, licenciamento, garantia do fabricante, suporte técnico especializado, implantação da solução, critérios de recebimento e condições de pagamento mostram-se compatíveis com aquelas normalmente praticadas no setor privado para soluções de segurança cibernética corporativa de elevada criticidade operacional.

A modelagem da contratação também observou os princípios da razoabilidade, proporcionalidade e vantajosidade administrativa, sem imposição de obrigações extraordinárias ou incompatíveis com as práticas usuais do mercado especializado de TIC.

Há manifestação sobre o atendimento do princípio da padronização?

Sim. A presente contratação observa o princípio da padronização previsto no art. 47, inciso I, da Lei nº 14.133/2021, considerando a necessidade de manutenção da arquitetura institucional de segurança cibernética atualmente implantada no IFRN.

A infraestrutura institucional de segurança da informação do IFRN encontra-se estruturada sobre solução integrada composta por equipamentos de firewall de próxima geração (NGFW) da fabricante Palo Alto Networks e pela plataforma de gerenciamento centralizado Palo Alto Panorama, já operacional em diversos campi da instituição.

A manutenção da padronização tecnológica visa assegurar:

- interoperabilidade plena entre os componentes da solução;
- gerenciamento centralizado da infraestrutura de segurança cibernética;
- reaproveitamento das políticas institucionais de segurança já configuradas;
- continuidade operacional dos serviços digitais institucionais;
- preservação dos investimentos públicos anteriormente realizados;
- redução de riscos operacionais decorrentes da coexistência de plataformas heterogêneas.

A adoção de solução tecnológica diversa implicaria significativa elevação da complexidade operacional, necessidade de substituição da infraestrutura de gerenciamento existente, reconstrução integral das políticas de segurança e aumento dos riscos relacionados à continuidade da operação institucional de TIC.

Há manifestação sobre o atendimento do princípio do parcelamento?

Sim. A presente contratação contempla manifestação expressa quanto ao atendimento do princípio do parcelamento previsto no art. 40 da Lei nº 14.133/2021, tendo sido tecnicamente justificada a adoção de grupo único para a solução pretendida.

O Estudo Técnico Preliminar demonstrou que a fragmentação do objeto comprometeria a integração operacional da solução de segurança cibernética institucional, a interoperabilidade entre os componentes tecnológicos e a adequada definição das responsabilidades técnicas relacionadas à implantação, suporte, gerenciamento e continuidade operacional da infraestrutura de TIC do IFRN.

A solução objeto da contratação possui natureza integrada, envolvendo equipamentos de firewall de próxima geração (NGFW), licenciamento, suporte técnico especializado, gerenciamento centralizado e serviços críticos de implantação e integração com a plataforma institucional Palo Alto Panorama, circunstância que exige uniformidade tecnológica e responsabilidade técnica centralizada.

A divisão do objeto em múltiplos contratos ou fornecedores poderia resultar em:

- fragmentação das responsabilidades técnicas;
- aumento da complexidade da gestão contratual;
- dificuldades de fiscalização;
- incompatibilidades operacionais;
- elevação dos riscos relacionados à segurança cibernética institucional;
- comprometimento da continuidade operacional dos serviços digitais do IFRN.

Dessa forma, o não parcelamento da solução encontra fundamento no art. 40, §3º, e no art. 47, inciso II, da Lei nº 14.133/2021, considerando a inviabilidade técnica da fragmentação da solução e a necessidade de preservação da integração operacional da infraestrutura institucional de segurança cibernética.

Há manifestação sobre a compatibilidade da despesa estimada com a prevista nas leis orçamentárias?

Sim. A presente contratação possui compatibilidade com as leis orçamentárias vigentes, em observância ao art. 18 da Lei nº 14.133/2021.

A demanda encontra-se prevista no Plano de Contratações Anual (PCA) do IFRN para o exercício de 2026 e alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) institucional, estando compatível com o planejamento estratégico, orçamentário e operacional da instituição.

A contratação visa atender necessidade institucional relacionada à continuidade operacional da infraestrutura de segurança cibernética, à proteção dos serviços digitais e à modernização da infraestrutura de TIC do IFRN, em consonância com as diretrizes estabelecidas na Lei Orçamentária Anual (LOA), na Lei de Diretrizes Orçamentárias (LDO) e no Plano Plurianual (PPA).

Consta informação do uso ou justificativa para não utilização de catálogo eletrônico de padronização?

Sim. Foi verificada a existência de catálogo eletrônico de padronização aplicável à presente contratação, nos termos do art. 19, inciso II, da Lei nº 14.133/2021.

Contudo, não foram identificados catálogos eletrônicos de padronização compatíveis de forma integral com as especificidades técnicas da solução de segurança cibernética institucional pretendida, especialmente quanto à infraestrutura de firewall de próxima geração (NGFW), interoperabilidade com a plataforma Palo Alto Panorama, requisitos de gerenciamento centralizado, segurança cibernética e continuidade operacional da infraestrutura institucional de TIC do IFRN.

Em razão das características técnicas especializadas da solução, a especificação dos requisitos da contratação foi realizada com base nas necessidades institucionais identificadas no Estudo Técnico Preliminar, observando os princípios da padronização, interoperabilidade, segurança da informação e vantagem administrativa.

Caso haja indicação de marca ou modelo, consta justificativa para a indicação?

Sim. A indicação da fabricante Palo Alto Networks encontra-se tecnicamente justificada nos autos, em observância ao art. 41, inciso I, da Lei nº 14.133/2021.

A justificativa decorre da necessidade de manutenção da padronização tecnológica da infraestrutura institucional de segurança cibernética do IFRN, atualmente estruturada sobre solução integrada composta por appliances NGFW da fabricante Palo Alto Networks e pela plataforma de gerenciamento centralizado Palo Alto Panorama, já implantada e operacional em diversos campi da instituição.

O Estudo Técnico Preliminar demonstrou que a adoção de solução de fabricante diverso implicaria:

- perda de interoperabilidade nativa com a infraestrutura existente;
- necessidade de substituição da solução de gerenciamento centralizado;
- reconstrução integral das políticas institucionais de segurança;
- aumento da complexidade operacional;
- elevação dos riscos relacionados à continuidade da infraestrutura institucional de TIC;
- necessidade de novos investimentos em capacitação técnica e migração tecnológica;
- fragmentação da gestão da segurança cibernética institucional.

A indicação da plataforma tecnológica também se fundamenta na necessidade de:

- continuidade operacional;
- gerenciamento centralizado;
- reaproveitamento dos investimentos públicos já realizados;
- uniformidade tecnológica;
- preservação da segurança cibernética institucional;
- redução de riscos operacionais decorrentes da coexistência de plataformas heterogêneas.

Dessa forma, a indicação da fabricante encontra respaldo técnico e jurídico no princípio da padronização previsto no art. 47, inciso I, da Lei nº 14.133/2021, bem como nas hipóteses admitidas pelo art. 41, inciso I, da referida Lei.

Há certificação no ETP ou nos autos de que a opção pela aquisição é mais vantajosa do que eventuais alternativas, como a locação de bens?

Sim. Durante o levantamento das alternativas tecnológicas foi avaliada a viabilidade de modelos alternativos de contratação, incluindo locação de equipamentos e soluções baseadas exclusivamente em subscrição de serviços.

Concluiu-se que a aquisição da solução mostra-se mais vantajosa para a Administração Pública, considerando as características permanentes da infraestrutura institucional de segurança cibernética do IFRN, a necessidade de continuidade operacional da arquitetura tecnológica implantada e o ciclo de vida esperado dos equipamentos NGFW.

A opção pela aquisição permite:

- preservação dos investimentos públicos realizados em infraestrutura de segurança institucional;
- maior previsibilidade orçamentária ao longo do ciclo de vida da solução;
- redução de custos recorrentes de locação;
- manutenção da padronização tecnológica institucional;
- continuidade operacional da solução de gerenciamento centralizado já implantada;
- maior autonomia administrativa na gestão da infraestrutura institucional de TIC.

Adicionalmente, verificou-se que modelos de locação ou subscrição integral poderiam gerar dependência operacional mais elevada, custos recorrentes continuados superiores ao longo do tempo e maior complexidade contratual para gestão da solução institucional de segurança cibernética.

Dessa forma, concluiu-se pela maior vantajosidade técnica e econômica da aquisição da solução pretendida, considerando o ciclo de vida da infraestrutura, os custos totais de propriedade (TCO) e as necessidades permanentes de segurança cibernética do IFRN.

17. Benefícios a serem alcançados com a contratação

A contratação de equipamentos de firewall de próxima geração (NGFW) da fabricante Palo Alto Networks proporcionará ao Instituto Federal do Rio Grande do Norte – IFRN uma série de benefícios institucionais relevantes, com impacto direto na operação dos serviços de tecnologia da informação, na proteção dos ativos da sua infraestrutura computacional e na qualidade do atendimento prestado à comunidade acadêmica e administrativa. Os principais benefícios são:

- Aumento da disponibilidade dos sistemas institucionais ao reduzir o risco de falhas e indisponibilidades, assegurando a continuidade das atividades acadêmicas e administrativa.
- Melhoria na capacidade de resposta a incidentes de segurança com a adoção de recursos avançados de prevenção de ameaças, filtragem de tráfego e inspeção de aplicações, permitindo proteção proativa contra ataques cibernéticos e redução do tempo de repostas.
- Aumento da produtividade da equipe técnica, por meio da padronização com a solução já dominada pelos profissionais de TIC do IFRN, o que reduz a curva de aprendizado, simplifica a gestão e evita retrabalho em processos de configuração, suporte e monitoramento.
- Preservação dos investimentos já realizados pelo Instituto Federal, evitando a necessidade de aquisição de novas ferramentas de gerenciamento, reconfiguração de ambientes ou capacitação adicional, atendendo aos princípios da economicidade.

- Modernização da infraestrutura de TIC com escalabilidade e sustentabilidade, ao adquirir equipamentos com capacidade de processamento e recursos avançados de segurança.

18. Providências a serem Adotadas

Não foram identificadas providências prévias necessárias, além das medidas operacionais padrão relacionadas ao recebimento dos equipamentos e à fiscalização da execução contratual.

19. Impactos ambientais e medidas de sustent

IMPACTOS AMBIENTAIS E MEDIDAS DE SUSTENTABILIDADE

A contratação observará, sempre que aplicável, critérios de sustentabilidade relacionados à eficiência energética dos equipamentos, maior vida útil dos ativos de TIC, redução do consumo energético e descarte ambientalmente adequado dos equipamentos substituídos, em conformidade com as diretrizes do Guia Nacional de Contratações Sustentáveis da AGU.

A adoção de solução padronizada também contribui para a racionalização da infraestrutura tecnológica institucional, redução de retrabalho operacional e ampliação do ciclo de vida dos ativos atualmente implantados.

20. Declaração de Viabilidade

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

20.1. Justificativa da Viabilidade

Após a análise detalhada das necessidades do Instituto Federal do Rio Grande do Norte – IFRN, das soluções disponíveis no mercado e dos benefícios esperados com a contratação, conclui-se pela viabilidade da Solução 1: Aquisição de firewalls do mesmo fabricante já utilizado pelo IFRN como a melhor alternativa para atender às demandas de segurança cibernética da instituição.

O estudo técnico preliminar demonstrou que a alternativa mais adequada para atender às necessidades do Instituto Federal do Rio Grande do Norte – IFRN é a aquisição de equipamentos de firewall de próxima geração (NGFW) da mesma fabricante já utilizada pela instituição, a Palo Alto Networks.

A solução escolhida proporcionará benefícios para o IFRN que estão alinhados aos princípios da administração pública e aos objetivos estratégicos da instituição, conforme descritos a seguir:

- A contratação assegura a entrega dos equipamentos e serviços com aderência aos requisitos técnicos e operacionais definidos e compatíveis às necessidades do Instituto Federal, contribuindo para a manutenção e a expansão segura da infraestrutura de TIC do IFRN;
- A continuidade da solução em uso permitirá uma proteção eficiente da rede, a disponibilidade dos sistemas e a prevenção de incidentes de segurança, viabilizando o cumprimento da missão institucional do Instituto Federal;
- Ao manter a plataforma tecnológica já dominada pela equipe técnica e plenamente integrada à arquitetura atual, o IFRN otimiza o uso dos recursos disponíveis, reduz retrabalho, evita gastos com novos treinamentos e garante maior agilidade nas ações de gestão e resposta a incidentes;
- A escolha evita investimentos duplicados em licenças, softwares de gerenciamento, reconfigurações e capacitações, maximizando o aproveitamento dos recursos públicos já empregados na infraestrutura vigente e assegurando a melhor relação entre custo e benefício ao longo do ciclo de vida da solução.

Portanto, declara-se a viabilidade da contratação de equipamentos de firewall de próxima geração (NGFW) da fabricante Palo Alto Networks, considerando seus benefícios técnicos, econômicos e estratégicos, alinhados aos objetivos institucionais do Instituto Federal do Rio Grande do Norte – IFRN e às melhores práticas de segurança cibernética.

21. 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](#).

JOAO RODRIGO SILVA DE CARVALHO

Membro da comissão de contratação



Assinou eletronicamente em 24/08/2026 às 09:55:42.

FRANCISCA SIMONELY DE VASCONCELOS

Membro da comissão de contratação



Assinou eletronicamente em 24/08/2026 às 09:38:34.

Despacho: Aprovo o presente Estudo Técnico Preliminar, nos termos da IN SGD nº 94/2022, declarando sua conformidade técnica e autorizando o prosseguimento da contratação.

TARSO LATORRACA CASADEI

Autoridade Máxima da Área de TIC



Assinou eletronicamente em 24/08/2026 às 09:56:00.

Despacho: Aprovo o Estudo Técnico Preliminar, considerando sua adequação técnica e a necessidade da contratação, autorizando a continuidade do processo conforme fundamentado nos autos.

ROBERTO GOMES CAVALCANTE JUNIOR

Autoridade competente



Assinou eletronicamente em 24/08/2026 às 10:35:47.

Documento Digitalizado Público

ETP158155_000141_2026

Assunto: ETP158155_000141_2026
Assinado por: Simonely Vasconcelos
Tipo do Documento: Estudo Técnico Preliminar
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Cópia Simples

Documento assinado eletronicamente por:

■ **Francisca Simonely de Vasconcelos, Coordenadora de Compras - SUB-CHEFIA - COCOMP/DILIC**, em 24/08/2026 11:18:19.

Este documento foi armazenado no SUAP em 24/08/2026. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifrn.edu.br/verificar-documento-externo/> e forneça os dados abaixo:

Código Verificador: 2698693
Código de Autenticação: 317bfee94c

