

Termo de Referência 133/2026

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
133/2026	158155-INST.FED.DE EDUC.,CIENC.E TEC.DO R.G.DO NORTE	FRANCISCA SIMONELY DE VASCONCELOS	24/08/2026 10:39 (v 0.3)
Status	ASSINADO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
V - prestação de serviços, inclusive os técnico-profissionais especializados/Serviço não-continuado	204/2026	23421.002414.2026-65

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. A presente licitação tem por objeto o Registro de Preços para contratação de solução de firewall de próxima geração destinada à segurança da informação e à proteção do perímetro da rede, proporcionando visibilidade e controle de tráfego e aplicações em camada 7, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas, filtragem de dados, VPN e controle granular de banda de rede, compreendendo o fornecimento de equipamentos, softwares integrados em forma de appliance, licenciamento, garantia, suporte técnico do fabricante e serviços especializados de instalação, configuração, integração e implantação da solução, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

<u>Lote</u>	<u>Item</u>	<u>Especificação</u>	<u>CATMAT/</u> <u>CATSER</u>	<u>Métrica ou</u> <u>Unidade</u> <u>de Medida</u>	<u>Qnt.</u>	<u>Valor Unitário</u>	<u>Valor Total</u>
<u>1</u>	<u>1</u>	<u>Solução de Firewall de Próxima Geração - Tipo I (campi)</u>	<u>609340</u>	<u>Unidade</u>	<u>27</u>	<u>R\$ 43.237,61</u>	<u>R\$ 1.167.415,47</u>
	<u>2</u>	<u>Solução de Firewall de Próxima Geração - Tipo II (datacenter)</u>	<u>609340</u>	<u>Unidade</u>	<u>2</u>	<u>R\$ 866.265,31</u>	<u>R\$ 1.732.530,62</u>
	<u>3</u>	<u>Serviço de Instalação e Configuração da Solução de Firewall de Próxima Geração</u>	<u>27014</u>	<u>Serviço</u>	<u>27</u>	<u>R\$ 52.207,56</u>	<u>R\$ 1.409.604,12</u>

	<u>4</u>	<u>Banco de Horas de 20 Horas de Serviço Técnico Especializado</u>	<u>27340</u>	<u>Serviço</u>	<u>5</u>	<u>R\$ 10.914,50</u>	<u>R\$ 54.572,50</u>
						<u>Valor Total</u>	<u>R\$ 4.364.122,71</u>

1.2. Estimativas de consumo individualizadas, do órgão gerenciador e órgão(s) e entidade(s) participante(s).

<u>Item</u>	<u>Descrição/ especificação</u>	<u>Unidade de medida</u>	<u>Requisição mínima</u>	<u>Requisição máxima</u>	<u>Quantidade total</u>
<u>1</u>	<u>Solução de Firewall de Próxima Geração - Tipo I (campi)</u>	<u>Unidade</u>	<u>10</u>	<u>27</u>	<u>27</u>
<u>2</u>	<u>Solução de Firewall de Próxima Geração - Tipo II (datacenter)</u>	<u>Unidade</u>	<u>1</u>	<u>2</u>	<u>2</u>
<u>3</u>	<u>Serviço de Instalação e Configuração da Solução de Firewall de Próxima Geração</u>	<u>Serviço</u>	<u>10</u>	<u>27</u>	<u>27</u>
<u>4</u>	<u>Banco de Horas de 20 Horas de Serviço Técnico Especializado</u>	<u>Serviço</u>	<u>1</u>	<u>5</u>	<u>5</u>

Classificação do objeto quanto à heterogeneidade ou complexidade

1.3. Os bens objeto desta contratação são caracterizados como comuns, uma vez que possuem padrões de desempenho e qualidade, bem como características gerais e específicas usualmente encontradas no mercado. Estes bens podem ser objetivamente definidos pelo edital, com especificações e características descritas no termo de referência. Os licitantes, de posse destas especificações, podem cotar preços oferecendo itens que já se encontram disponíveis de forma padronizada no mercado atual. Em função destas características, estes bens podem ser comercializados por processo licitatório na modalidade pregão em sua forma eletrônica, conforme dispõe os incisos XIII e XLI do artigo 6º da Lei nº 14.133/2021.

Classificação do objeto como bem de luxo

1.5. O objeto desta contratação não se enquadra como bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

Prazo de vigência

1.7. O prazo de vigência da contratação é de 12 (doze) meses, contados da data de assinatura do contrato pelas partes, na forma do art. 105 da Lei nº 14.133, de 2021.

1.11. O contrato ou outro instrumento hábil que o substitua oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. 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.

2.2. A presente contratação é motivada pela necessidade de expansão, modernização e padronização da infraestrutura de segurança de rede do IFRN, 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).

2.3. 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.

2.4. A contratação de novos equipamentos NGFW compatíveis com a solução da Palo Alto Networks já utilizada pela IFRN possibilita o aproveitamento de investimentos já realizados pela Administração, incluindo infraestrutura de gerenciamento, processos operacionais consolidados e capacitação da equipe técnica, evitando dispêndios adicionais desnecessários. 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.

2.5. 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.

2.6. A definição das quantidades de equipamentos e serviços considerou os critérios de obsolescência de equipamentos existentes e a necessidade de cobertura de novos campi. As quantidades foram estimadas no estudo técnico preliminar para compor o projeto em sua totalidade. 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 IFRN.

2.7. A adoção do Sistema de Registro de Preços mostra-se adequada em razão da possibilidade de execução gradual da implantação da solução nos diversos campi do IFRN, permitindo que as aquisições ocorram conforme disponibilidade orçamentária e cronograma institucional de implantação, sem a necessidade de contratação integral imediata.

2.8. A Ata de Registro de Preços terá vigência de 12 (doze) meses, contados da sua assinatura, podendo ser prorrogada por igual período, desde que comprovada a vantajosidade dos preços registrados, nos termos do art. 84 da Lei nº 14.133/2021 e do Decreto nº 11.462/2023. Os quantitativos registrados constituem estimativa da demanda, não gerando obrigação de contratação integral pela Administração.

2.9. Será admitida a adesão à Ata de Registro de Preços por órgãos ou entidades não participantes, observados os requisitos, procedimentos e limites estabelecidos no art. 86 da Lei nº 14.133/2021 e no Decreto nº 11.462/2023. A

eventual adesão ficará condicionada à prévia anuência do IFRN, na condição de órgão gerenciador, e à aceitação do fornecedor beneficiário da ata, bem como ao atendimento das demais condições previstas na legislação aplicável.

2.10. A solução contempla equipamentos e serviços amplamente utilizados na Administração Pública Federal para proteção de ambientes corporativos de TIC, possuindo potencial de atendimento a demandas semelhantes de instituições federais de ensino, pesquisa e administração pública.

2.11. O objeto da contratação está previsto no Plano de Contratações Anual **2026**, conforme detalhamento a seguir:

- I) ID PCA no PNCP: **10877412000168-0-000002/2026;**
- II) Data de publicação no PNCP: **25/03/2025;**
- III) Id do item no PCA: **685, 686,687 e 688;**
- IV) Classe/Grupo: **162 - SERVIÇOS DE GERENCIAMENTO EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC); 173 - SERVIÇOS DE CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC); 7050 - EQUIPAMENTOS DE REDE DE TIC - LOCAL E REMOTA;**
- V) Identificador da Futura Contratação: **158155-166/2026;**

ALINHAMENTO AO PCA 2026	
ITEM	DESCRIÇÃO
310	<u>UASG: 158155 – Reitoria do IFRN</u> <u>Categoria: Solução de TIC</u> <u>Classificação: 182 - SERVIÇOS DE LICENCIAMENTO E CONTRATOS DE TRANSFERÊNCIA DE TECNOLOGIA</u> <u>Valor Total Estimado: R\$ 558.890,00</u> <u>Data Prevista para Contratação: 30/11/2026</u>
320	<u>UASG: 158155 – Reitoria do IFRN</u> <u>Categoria: Solução de TIC</u> <u>Classificação: 7090 - SUPRIMENTOS DE INFORMÁTICA - TIC</u> <u>Valor Total Estimado: R\$ 1.400.000,00</u> <u>Data Prevista para Contratação: 30/11/2026</u>
621	<u>UASG: 158155 – Reitoria do IFRN</u> <u>Categoria: Solução de TIC</u> <u>Classificação: 7090 - SUPRIMENTOS DE INFORMÁTICA - TIC</u> <u>Valor Total Estimado: R\$ 1.400.000,00</u> <u>Data Prevista para Contratação: 30/11/2026</u>
31	<u>UASG: 158155 – Reitoria do IFRN</u> <u>Categoria: Serviço</u> <u>Classificação: 165 - SERVICOS PARA A INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC), NAO CLASSIFICADOS EM OUTROS TÓPICOS</u> <u>Valor Total Estimado: R\$ 120.000,00</u> <u>Data Prevista para Contratação: 30/11/2026</u>

2.12. O objeto da contratação também está alinhado com a Estratégia de Governo Digital **2026** e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	Objetivos Estratégicos
<u>GI-4</u>	<u>Consolidar a gestão de TI</u>

ALINHAMENTO AO PDTIC <u>2021-2024*</u>			
ID	Ação do PDTIC	ID	Meta do PDTIC associada
<u>A1</u>	<u>Realizar levantamento de necessidade de atualização dos equipamentos de datacenter</u>	<u>M19</u>	<u>Manter atualizados os equipamentos de datacenter.</u>
<u>*Conforme Justificativa Técnica e Legal para Contratações de TIC na Ausência de PDTIC Vigente (Ofício Nº 16/2025 - DIGTI/RE/IFRN)</u>			

2.13. Por tratar de oferta de serviços públicos digitais, o objeto da contratação será integrado à Plataforma Gov.br, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, e suas atualizações, de acordo com as especificações deste Termo de Referência.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3.2. A solução de TIC consiste em na contratação de uma solução de firewall de próxima geração (Next Generation Firewall - NGFW) para segurança da informação e proteção do perímetro da rede proporcionando a visibilidade e controle de tráfego e aplicações em camada 7, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos e softwares integrados em forma de appliance.

3.3. Considerando as necessidades do IFRN em implementar uma solução robusta para proteger sua infraestrutura de TI contra ataques cibernéticos, as quantidades e especificações foram definidas no estudo técnico preliminar. Essas definições asseguram que o projeto atenda integralmente à infraestrutura de TIC da instituição, cobrindo todos os seus campi e garantindo a proteção e a continuidade das operações acadêmicas e administrativas.

3.4. DESCRIÇÃO DETALHADA DA SOLUÇÃO DE TIC

3.4.1. Solução de Firewall de Próxima Geração - Tipo I

<u>LOTE</u>	<u>ITEM</u>	<u>DESCRIÇÃO</u>

Solução de Firewall de Próxima Geração - Tipo I (campi)Características técnicas mínimas:

1. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN;
2. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
3. O equipamento deve ser fornecido com kit que permita a sua montagem em rack 19";
4. Deve possuir throughput de, no mínimo, 2 (dois) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;
5. Deve possuir throughput de, no mínimo, 1 (um) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos;
6. Deve suportar, no mínimo, 180.000 (cento e oitenta mil) conexões simultâneas;
7. Deve suportar, no mínimo, 30.000 (trinta mil) novas conexões por segundo;
8. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1 Gbps do tipo RJ-45;
9. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento;
10. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;
11. Deve possuir, no mínimo, 120 (cento e vinte) GB de armazenamento interno para o sistema operacional;
12. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento;
13. Deve suportar, no mínimo, 800 (oitocentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;
14. Deve suportar, no mínimo, 500 (quinhentos) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;
15. Deve possuir suporte a criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 1.000 (hum mil) VLANs;
16. Deve implementar o protocolo LLDP – Link Layer Discovery Protocol;
17. Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um link agrupado virtualmente (LAG – Link Aggregation Group);
18. Deve possuir o recurso de NAT – Network Address Translation nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso deve ser aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (Network Prefix Translation) para tradução de um prefixo IPv6 para outro prefixo IPv6 prevenindo problemas de roteamento assimétrico;
19. Deve suportar a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF graceful restart e BGP;
20. Deve implementar o protocolo ECMP – Equal Cost Multiple Path para balanceamento de carga entre links baseados no hash do endereço IP de origem, no hash do endereço IP de origem e de destino, pela técnica conhecida como round-robin e com base no peso ou prioridade atribuído a cada link. Deve suportar o balanceamento entre, no mínimo, 2 (dois) links;
21. Deve permitir o envio de logs para sistemas de monitoração externos utilizando

o padrão syslog, bem como o envio de forma segura através do protocolo SSL/TLS;

22. Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo;

23. Deve implementar controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego;

24. A identificação do país deve ser através do código do país, por exemplo, BR, USA, UK, RUS, etc e também através de geolocalização possibilitando a criação de regiões geográficas;

25. Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;

26. Deve possuir a capacidade para realizar a descriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A descriptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego;

27. Deve possuir recurso de QoS – Quality of Service com suporte a DSCP – Differentiated Services Code Point. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação;

28. Deve possuir a capacidade de reconhecer, no mínimo, 5.000 (cinco mil) aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, peer-to-peer, sistemas de mensagem instantânea, etc, sendo esta uma lista não exaustiva;

29. O reconhecimento da aplicação se dará, independentemente de porta e protocolo, através de, no mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da solução de firewall, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado;

30. Deve permitir a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante;

31. Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação;

32. Deve permitir bloquear sessões TCP que utilizarem variações do three-way handshake como four-way e o five-way split handshake, prevenindo assim possíveis tráfegos maliciosos;

33. Deve permitir bloquear conexões que contenham dados no payload dos pacotes TCP SYN e TCP SYN-ACK durante o three-way handshake;

34. A solução de firewall deve possuir funcionalidades de IPS, antivírus e anti-spyware que permita o bloqueio de vulnerabilidades e exploits conhecidos e proteção contra vírus e spywares baseado em assinaturas de ameaças conhecidas;

35. Deve ser possível a criação de assinaturas customizadas de ameaças;

36. Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de appliance externo para o bloqueio de vírus caso a solução de firewall ofertada não realize nativamente a inspeção em algum dos protocolos solicitados;

37. Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;

38. Deve possuir proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN Flood, ICMP Flood, UDP Flood, etc e deve também bloquear port scans, bloquear ataques de buffer overflow e identificar e bloquear comunicação com botnets;

39. Para cada ameaça detectada pela solução deve ser realizado o registro nos logs do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego);
40. A solução de firewall deve possuir funcionalidade para análise, em tempo real através de mecanismos de Machine Learning, de ameaças de comando e controle (C2) desconhecidas, sendo capaz de monitorar e bloquear a comunicação através de, no mínimo, os protocolos HTTP, HTTP/2, SSL e ataques realizados por meio de aplicações desconhecidas tanto em tráfego TCP quanto UDP;
41. A solução de firewall deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a websites baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP;
42. A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;
43. Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;
44. Deve prover análise, em tempo real através de mecanismos de Machine Learning, dos websites acessados pelos usuários realizando a inspeção do seu conteúdo, detectando assim conteúdos que possam ser uma ameaça e realizando a categorização da URL como maliciosa e bloqueando tal URL, mesmo que ela não esteja presente e devidamente categorizada na base de dados de URL da solução;
45. Deve permitir a customização da página de bloqueio exibida ao usuário quando o mesmo tentar realizar um acesso a um website pertencente a uma categoria de URLs bloqueada;
46. Deve possuir recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o Active Directory, submetidas em sites não corporativos. Deve ser possível definir em quais websites é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o website pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao Active Directory em um website não autorizado deve ser exibido no web browser do mesmo uma página de bloqueio informando que o uso de tais credenciais no website específico não está autorizado;
47. A solução de firewall deve possuir recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e também definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de web browser. Deve permitir bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent;
48. A solução de firewall deve possuir integração com LDAP, MS Active Directory e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas /regras baseadas por usuários e grupo de usuários;
49. A integração com MS Active Directory para identificação dos usuários da rede deve ser realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários;
50. A solução de firewall deve possuir recurso de portal de autenticação prévia (Captive Portal) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de software cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;
51. A solução de firewall deve possuir o recurso de VPN – Virtual Private Network dos tipos site-to-site e client-to-site e suportar IPSEC – Internet Protocol Security e SSL – Secure Sockets Layer;
52. O recurso de VPN IPSEC deve suportar os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5 e SHA 1, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves Diffie-Hellman Grupo 1,

Grupo 2, Grupo 5 e Grupo 14 e suportar também a autenticação através de certificados IKE PKI;

53. O recurso de VPN SSL deve permitir que o usuário remoto se conecte através de um software cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo;

54. Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a autenticação via certificado e OTP – One Time Password;

55. Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional MS Windows 10 e superior e MacOS 14 e superior;

56. A solução de firewall deve possuir console de gerenciamento do equipamento acessada através de interface gráfica web permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e anti-spyware, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de logs de eventos e demais configurações;

57. Deve suportar a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS Active Directory, RADIUS e através de base de usuários local no equipamento da solução de firewall;

58. Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros;

59. Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;

60. A interface de gerenciamento do equipamento deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regras (shadowing) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve possuir também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão da mesma para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente. É permitido o uso de appliance externo para realização da análise das políticas;

61. Deve ser possível através de interface de gerenciamento do equipamento a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuário específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados;

62. Deve ser possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – Software as a Service mostrando os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso a aplicação SaaS e o consumo da aplicação SaaS pelo usuário;

63. Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;

64. Deve ser possível configurar o envio de alertas do sistema via e-mail;

65. Deve suportar o monitoramento via SNMPv3;

66. O sistema operacional a ser instalado no equipamento que compõe a solução deverá ser fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico;

67. Por cada equipamento que compõe a solução de segurança, entende-se o

hardware e as licenças de softwares necessárias para o seu funcionamento;

68. A Solução de Firewall de Próxima Geração ofertada deve ser homologada e totalmente compatível com o software de gerenciamento centralizado Palo Alto Panorama atualmente instalado e em operação no IFRN;

69. Na data do certame, nenhum dos equipamentos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

70. Durante o período de vigência do contrato de garantia todos os componentes da solução de firewall, incluindo o equipamento, o sistema operacional do mesmo, as licenças necessárias para atender as funcionalidades e recursos solicitados, os softwares clientes de VPN e demais itens necessários para o perfeito funcionamento devem estar cobertos por garantia e suporte técnico do fabricante da solução em caso de problema;

71. A solução de firewall deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e dos demais software e das assinaturas de proteção da solução.

3.4.2. Solução de Firewall de Próxima Geração - Tipo II

<u>LOTE</u>	<u>ITEM</u>	<u>DESCRIÇÃO</u>
<u>1</u>	<u>2</u>	<u>Solução de Firewall de Próxima Geração - Tipo II (datacenter)</u> <u>Características técnicas mínimas:</u> <u>1. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN;</u> <u>2. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;</u> <u>3. O equipamento fornecido deve ser próprio para montagem em rack 19", incluindo kit para fixação em rack 19", se necessário, e cabos de alimentação;</u> <u>4. Deve possuir throughput de, no mínimo, 9 (nove) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;</u> <u>5. Deve possuir throughput de, no mínimo, 6 (seis) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos;</u> <u>6. Deve suportar, no mínimo, 1.200.000 (um milhão e duzentos mil) sessões simultâneas;</u> <u>7. Deve suportar, no mínimo, 120.000 (cento e vinte mil) novas sessões por segundo;</u> <u>8. Deve possuir, no mínimo, 12 (doze) interfaces físicas de rede de 1 Gbps do tipo RJ-45;</u> <u>9. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 10 Gbps do tipo SFP+;</u> <u>10. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps do tipo RJ-45 dedicada e exclusiva para gerenciamento;</u> <u>11. Deve possuir, no mínimo, 1 (uma) interface física de 10 Gbps do tipo SFP+ dedicada e exclusiva para o recurso de alta disponibilidade;</u> <u>12. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;</u> <u>13. Deve possuir, no mínimo, 240 (duzentos e quarenta) GB de armazenamento interno para o sistema operacional;</u> <u>14. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre</u>

- 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento (hot-swappable);
15. Deve suportar, no mínimo, 1.200 (um mil e duzentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;
16. Deve suportar, no mínimo, 1.000 (um mil) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;
17. Deve possuir suporte a criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 1.000 (um mil) VLANs;
18. Deve implementar o protocolo LLDP – Link Layer Discovery Protocol;
19. Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um link agrupado virtualmente (LAG – Link Aggregation Group);
20. Deve possuir o recurso de NAT – Network Address Translation nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso deve ser aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (Network Prefix Translation) para tradução de um prefixo IPv6 para outro prefixo IPv6 prevenindo problemas de roteamento assimétrico;
21. Deve suportar a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF graceful restart e BGP;
22. Deve implementar o protocolo ECMP – Equal Cost Multiple Path para balanceamento de carga entre links baseados no hash do endereço IP de origem, no hash do endereço IP de origem e de destino, pela técnica conhecida como round-robin e com base no peso ou prioridade atribuído a cada link. Deve suportar o balanceamento entre, no mínimo, 2 (dois) links;
23. Deve permitir o envio de logs para sistemas de monitoração externos utilizando o padrão syslog, bem como o envio de forma segura através do protocolo SSL/TLS;
24. Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo;
25. Deve implementar controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego;
26. A identificação do país deve ser através do código do país, por exemplo, BR, USA, UK, RUS, etc e também através de geolocalização possibilitando a criação de regiões geográficas;
27. Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;
28. Deve possuir a capacidade para realizar a decriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A decriptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego;
29. Deve possuir recurso de QoS – Quality of Service com suporte a DSCP – Differentiated Services Code Point. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação;
30. Deve possuir a capacidade de reconhecer, no mínimo, 5.000 (cinco mil) aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, peer-to-peer, sistemas de mensagem instantânea, etc, sendo esta uma lista não exaustiva;
31. O reconhecimento da aplicação se dará, independentemente de porta e

protocolo, através de, no mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da solução de firewall, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado;

32. Deve permitir a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante;

33. Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação;

34. Deve permitir bloquear sessões TCP que utilizarem variações do three-way handshake como four-way e o five-way split handshake, prevenindo assim possíveis tráfegos maliciosos;

35. Deve permitir bloquear conexões que contenham dados no payload dos pacotes TCP SYN e TCP SYN-ACK durante o three-way handshake;

36. A solução de firewall deve possuir funcionalidades de IPS, antivírus e anti-spyware que permita o bloqueio de vulnerabilidades e exploits conhecidos e proteção contra vírus e spywares baseado em assinaturas de ameaças conhecidas;

37. Deve ser possível a criação de assinaturas customizadas de ameaças;

38. Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de appliance externo para o bloqueio de vírus caso a solução de firewall ofertada não realize nativamente a inspeção em algum dos protocolos solicitados;

39. Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;

40. Deve possuir proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN Flood, ICMP Flood, UDP Flood, etc e deve também bloquear port scans, bloquear ataques de buffer overflow e identificar e bloquear comunicação com botnets;

41. Para cada ameaça detectada pela solução deve ser realizado o registro nos logs do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego);

42. A solução de firewall deve possuir funcionalidade para análise, em tempo real através de mecanismos de Machine Learning, de ameaças de comando e controle (C2) desconhecidas, sendo capaz de monitorar e bloquear a comunicação através de, no mínimo, os protocolos HTTP, HTTP/2, SSL e ataques realizados por meio de aplicações desconhecidas tanto em tráfego TCP quanto UDP;

43. A solução de firewall deve possuir a capacidade de detectar e bloquear tentativas de resolução de domínios gerados de forma automática através de algoritmos (Domain Generation Algorithm - DGA);

44. A solução de firewall deve possuir recurso de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle. A análise automática deve incluir, no mínimo, as seguintes características: a) Padrões de consulta; b) Entropia; c) Análise de frequência n-gram de domínios; d) Taxa de consultas.

45. A solução de firewall deve suportar a inspeção do tráfego DNS, incluindo os protocolos DNS-over-TLS (DoT) e DNS-over-HTTP (DoH);

46. Deve possuir a capacidade de detectar em tempo real ataques de resposta de DNS, como os tipos: DNS injection, DNS spoofing, DNS cache poisoning, domínios não resolvíveis, registrador de domínios (Registrar) comprometido e configurações erradas no DNS;

47. A solução de firewall deve possuir funcionalidade para análise, em tempo real através de mecanismos de Machine Learning, dos dados de requisição e respostas de DNS para detectar e bloquear respostas maliciosas ou alteradas;

48. A solução de firewall deve possuir funcionalidade para análise de malwares não conhecidos (Malware Zero Day) onde o dispositivo envia o arquivo de forma

automática para análise na “cloud” ou em um appliance instalado na rede local onde o arquivo será executado e simulado em um ambiente controlado (sandbox);

49. Caso seja necessário licença de sistema operacional e software para execução de arquivos no ambiente controlado (sandbox) as mesmas devem ser fornecidas em sua totalidade para o seu perfeito funcionamento;

50. O resultado da análise de malwares não conhecidos deve ter a capacidade de categorizar o arquivo analisado como, no mínimo, um arquivo malicioso, um arquivo não malicioso e um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema;

51. A análise de malwares não conhecidos deve ser realizada em arquivos trafegados na internet através dos protocolos HTTP, HTTPS e FTP bem como em arquivos trafegados entre servidores de arquivos utilizando o protocolo SMB. A análise também deve ser realizada em arquivos anexos em e-mails e links HTTP e HTTPS presentes no corpo de e-mails trafegados utilizando os protocolos SMTP e POP3. A análise do link HTTP e HTTPS presente no corpo do e-mail deve identificar se o website é um hospedeiro de exploits ou atividade de phishing;

52. Deve suportar a análise dos arquivos em ambientes controlados (sandbox) com, no mínimo, os sistemas operacionais MS Windows, MacOS e Linux;

53. Deve possuir capacidade de realizar análise inteligente de memória em tempo de execução para detecção de malwares residentes apenas em memória (fileless);

54. A análise de malwares não conhecidos em ambiente controlado (sandbox) deve ser realizada em arquivos tipo executáveis, DLLs, arquivos compactados RAR e 7-ZIP, arquivos do pacote MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos PDF, arquivos JAVA (.jar e class), arquivos DMG e PKG, arquivos ELF e arquivos APK;

55. A análise de malwares não conhecidos deve ser capaz de realizar, de forma complementar às assinaturas de antivírus, a inspeção inline em tempo real, através da utilização de Machine Learning no próprio firewall, em arquivos do tipo PE (Portable Executable), ELF (Executable and Linked Format), em arquivos Microsoft Office e em scripts PowerShell e shell script para detecção e proteção contra malwares desconhecidos;

56. A solução de firewall deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a websites baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP;

57. A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;

58. Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;

59. Deve prover análise, em tempo real através de mecanismos de Machine Learning, dos websites acessados pelos usuários realizando a inspeção do seu conteúdo, detectando assim conteúdos que possam ser uma ameaça e realizando a categorização da URL como maliciosa e bloqueando tal URL, mesmo que ela não esteja presente e devidamente categorizada na base de dados de URL da solução;

60. Deve permitir a customização da página de bloqueio exibida ao usuário quando o mesmo tentar realizar um acesso a um website pertencente a uma categoria de URLs bloqueada;

61. Deve possuir recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o Active Directory, submetidas em sites não corporativos. Deve ser possível definir em quais websites é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o website pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao Active Directory em um website não autorizado deve ser exibido no web browser do mesmo uma página de bloqueio informando que o uso de tais

credenciais no website específico não está autorizado;

62. A solução de firewall deve possuir recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e também definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de web browser. Deve permitir bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent;

63. A solução de firewall deve possuir integração com LDAP, MS Active Directory e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas /regras baseadas por usuários e grupo de usuários;

64. A integração com MS Active Directory para identificação dos usuários da rede deve ser realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários;

65. A solução de firewall deve possuir recurso de portal de autenticação prévia (Captive Portal) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de software cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;

66. A solução de firewall deve possuir recurso de portal de autenticação prévia (Captive Portal) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de software cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;

67. A solução deve fornecer uma arquitetura de segurança para dispositivos de IoT /OT baseada em inteligência artificial nativa. O perfilamento deve ser executado diretamente pelo firewall através de modelos de Machine Learning em três camadas (Categoria, Perfil e Instância), identificando mais de 1.600 atributos de identidade e postura, incluindo fabricante, modelo e versão de firmware, sem a necessidade de sensores de rede dedicados ou soluções de NAC externas para a classificação básica;

68. A solução deve oferecer mitigação proativa de riscos através de recomendações automáticas de políticas de Camada 7 adaptáveis, baseadas no comportamento real do dispositivo;

69. Deve possuir a capacidade nativa de Virtual Patching em linha, para ativos com vulnerabilidades críticas e sem suporte do fabricante, correlacionando automaticamente exploits conhecidos às assinaturas de prevenção de ameaças avançadas para proteger firmwares que não podem ser atualizados fisicamente;

70. A solução deve ainda monitorar continuamente o tráfego para detectar anomalias comportamentais e prever a probabilidade de exploração de vulnerabilidades (pontuação EPSS), integrando-se nativamente ao motor de IPS sem a necessidade de módulos de software ou hardware adicionais para a resposta a incidentes;

71. A solução de firewall deve possuir o recurso de VPN – Virtual Private Network dos tipos site-to-site e client-to-site e suportar IPSEC – Internet Protocol Security e SSL – Secure Sockets Layer;

72. O recurso de VPN IPSEC deve suportar os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5 e SHA 1, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14 e suportar também a autenticação através de certificados IKE PKI;

73. O recurso de VPN SSL deve permitir que o usuário remoto se conecte através de um software cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo;

74. Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a

autenticação via certificado e OTP – One Time Password;

75. Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional MS Windows 10 e superior e MacOS 14 e superior;

76. O recurso de VPN SSL deve possuir mecanismo de checagem da conformidade do computador do usuário remoto e a checagem deve permitir verificar, no mínimo, as informações de qual sistema operacional e patches estão instalados, se o antivírus está instalado e ativo no computador, se o firewall está instalado e ativo no computador, se o disco está criptografado, se o agente de DLP – Data Loss Prevention está instalado e ativo, informações de chaves de registro e processos ativos no computador;

77. Deve ser possível criar perfis customizados de conformidade com, no mínimo, as mesmas informações obtidas pelo mecanismo de checagem da conformidade do computador do usuário remoto. Tais perfis devem ser utilizados para assegurar que apenas computadores de usuários remotos que atendem aos requisitos solicitados nos perfis customizados possam ter acesso através da VPN aos dados e sistemas hospedados na rede interna do órgão;

78. A solução de firewall deve possuir console de gerenciamento do equipamento acessada através de interface gráfica web permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e anti-spyware, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de logs de eventos e demais configurações;

79. Deve suportar a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS Active Directory, RADIUS e através de base de usuários local no equipamento da solução de firewall;

80. Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros;

81. Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;

82. A interface de gerenciamento do equipamento deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regras (shadowing) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve possuir também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão da mesma para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente. É permitido o uso de appliance externo para realização da análise das políticas;

83. Deve ser possível através de interface de gerenciamento do equipamento a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuário específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados;

84. Deve ser possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – Software as a Service mostrando os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso a aplicação SaaS e o consumo da aplicação SaaS pelo usuário;

85. Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;

86. Deve ser possível configurar o envio de alertas do sistema via e-mail;

87. Deve suportar o monitoramento via SNMPv3;

88. O sistema operacional a ser instalado no equipamento que compõe a solução deverá ser fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico;
89. Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;
90. A Solução de Firewall de Próxima Geração ofertada deve ser homologada e totalmente compatível com o software de gerenciamento centralizado Palo Alto Panorama atualmente instalado e em operação no IFRN;
91. Na data do certame, nenhum dos equipamentos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
92. Durante o período de vigência do contrato de garantia todos os componentes da solução de firewall, incluindo o equipamento, o sistema operacional do mesmo, as licenças necessárias para atender as funcionalidades e recursos solicitados, os softwares clientes de VPN e demais itens necessários para o perfeito funcionamento devem estar cobertos por garantia e suporte técnico do fabricante da solução em caso de problema;
93. A solução de firewall deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e dos demais software e das assinaturas de proteção da solução.

3.4.3. Serviço de Instalação e Configuração da Solução de Firewall de Próxima Geração

LOTE	ITEM	DESCRIÇÃO
<u>1</u>	<u>3</u>	<u>Serviço de Instalação e Configuração da Solução de Firewall de Próxima Geração</u> <u>Características técnicas mínimas:</u> 1. A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos: 1.1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação; 1.2. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante. Deve considerar também a instalação em modo Alta Disponibilidade (ativo/passivo); 1.3. Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados; 1.4. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos; 1.5. Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7; 1.6. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução; 1.7. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e Anti-malware de acordo com as exigências levantadas; 2. Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls afim de garantir a melhor eficiência da solução durante o período de vigência das licenças; 3. As atividades de configuração da solução, migração de regras e demais

		atividades necessárias para a configuração do sistema poderão ser realizadas de forma remota;
		4. Adição do novo appliance de firewall no sistema de gerenciamento centralizado Palo Alto Panorama instalado e em operação no IFRN;
		5. Repasse de informação das configurações realizadas no formato hands-on de 4 horas para a equipe responsável pelo projeto por parte da contratante após validação da migração;

3.4.4. Banco de Horas de 20 Horas de Serviço Técnico Especializado

LOTE	ITEM	DESCRIÇÃO
1	4	<u>Banco de Horas de 20 Horas de Serviço Técnico Especializado</u> <u>Características técnicas mínimas:</u> 1. Banco de horas de 20 horas para prestação de serviço técnico especializado, de forma remota, a ser realizado nas soluções de firewall de próxima geração especificadas neste Termo de Referência; 2. O método de acesso remoto aos equipamentos será disponibilizado Contratante; 3. Os serviços de suporte técnico correspondem as seguintes atividades: 3.1. Sanar dúvidas relacionadas ao funcionamento e as funcionalidades dos equipamentos e softwares; 3.2. Realizar configurações ou ajustes e alterações das configurações existentes nos equipamentos; 3.3. Realizar a criação de novas regras de segurança nos equipamentos; 3.4. Realizar a revisão das regras de segurança e configurações dos equipamentos e softwares; 3.5. Emitir relatórios apontando potenciais problemas segurança e sugestões de melhorias nas configurações dos equipamentos; 3.6. Apoio técnico na instalação de atualizações de software/firmware disponibilizadas pelo fabricante; 4. Os serviços serão solicitados mediante a abertura de um chamado, por meio de correio eletrônico ou ferramenta web na Internet à contratada. A Contratada deverá indi-car os procedimentos para abertura do chamado de suporte técnico; 5. O atendimento deverá ser em idioma português do Brasil; 6. Deverá ser fornecido um número único de identificação do chamado no momento da abertura do chamado do serviço técnico especializado; 7. Todos os chamados, bem como as providências adotadas e o número de horas gastas no atendimento, deverão ser armazenados em sistema para controle de chamados da contratada; 8. O horário para abertura dos chamados deverá ser pelo menos das 08:00h às 18:00h (Horário de Brasília) em dias úteis (segunda a sexta-feira). O atendimento inicial deverá ocorrer em até 1 dia útil após a data de abertura do chamado;

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio

4.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

4.1.1. 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.

4.1.2. Preservar os investimentos já realizados pela instituição em tecnologia, capacitação e integração de sistemas.

4.1.3. Minimizar os riscos operacionais, de indisponibilidade e de segurança relacionados a uma atualização tecnológica.

4.1.4. Assegurar gerenciamento unificado e contínuo da segurança já implementado na rede do IFRN distribuída em seus diversos campi.

4.1.5. Promover a escalabilidade e a modernização da infraestrutura de segurança da solução atual de segurança do IFRN.

4.1.6. 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).

Requisitos de Capacitação

4.2. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação.

Requisitos Legais

4.3. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133, de 2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

Requisitos de Manutenção

4.4. Todos os itens deste processo devem possuir garantia do fabricante com validade mínima de 60 (sessenta) meses.

4.5. Os chamados poderão ser abertos ou diretamente com o fabricante ou com a autorizada oficial do fabricante no Brasil durante a vigência da garantia.

4.6. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs.

4.7. Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital, obedecendo à modalidade NBD (Next Business Day).

4.8. A empresa contratada deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico ou website ou e-mail.

4.9. A contratada deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana, com sistema de help desk para abertura de chamados de suporte técnico.

Requisitos Temporais

4.10. A Entrega dos equipamentos deverá ser efetivada no prazo máximo de **120 (cento e vinte) dias corridos** ~~para as capitais dos estados e de [xx] dias corridos para as demais localidades~~, a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

4.11. A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada.

4.12. Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local para download do arquivo de instalação.

4.13. O prazo para execução dos serviços de Instalação e Configuração do Firewall de Próxima Geração é de até 45 (quarenta e cinco) dias corridos a contar do recebimento dos equipamentos, podendo este prazo ser prorrogado por igual período a critério da Administração.

Requisitos de Segurança e Privacidade

4.14. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante, e:

4.14.1. Controle de Acesso: Implementação de contas de acesso únicas, pessoais e intransferíveis, com senhas seguras e temporárias, e bloqueio de contas após tentativas malsucedidas ou períodos de inatividade. Garantir que apenas usuários autorizados tenham acesso aos sistemas e dados do IFRN.

4.14.2. Monitoramento e Auditoria: Manutenção de registros de auditoria (logs) para monitorar atividades da rede, incluindo acessos remotos e utilização de VPN. Esses registros devem permitir o rastreamento das ações tomadas para posterior auditoria, garantindo a integridade e segurança das informações.

4.14.3. Acesso Remoto Seguro: Utilização de VPN para acesso remoto, com análise de riscos e autorização prévia. As conexões remotas devem ser seguras e monitoradas para evitar vulnerabilidades e garantir a proteção dos dados.

4.14.4. Garantia de Segurança, Integridade e Disponibilidade das Informações: Implementação de medidas de segurança para proteger contra ameaças cibernéticas, garantindo a integridade e disponibilidade das informações manipuladas pela solução. Isso inclui a utilização de soluções de detecção e bloqueio de programas maliciosos, como antispymware e antivírus.

4.14.5. Proteção à Privacidade dos Dados: Ampla proteção à privacidade dos dados do IFRN, conforme a Lei Geral de Proteção de Dados Pessoais (LGPD). Isso inclui o mapeamento de dados pessoais, a finalidade do tratamento desses dados, e a forma de atendimento aos direitos do titular, como acesso, retificação, exclusão e revogação de consentimento.

4.14.6. Sigilo nas Informações Acessadas: Garantir o sigilo das informações acessadas, assegurando que dados sensíveis sejam protegidos contra acessos não autorizados e vazamentos. A contratada deve seguir rigorosamente as normas de segurança da informação estabelecidas pelo IFRN.

Requisitos Sociais, Ambientais e Culturais

4.15. Os equipamentos devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

4.15.1. A documentação e os manuais da solução poderão ser apresentados no idioma Português (Brasil) ou no idioma Inglês.

Requisitos da Arquitetura Tecnológica

4.16 Os equipamentos deverão observar integralmente os requisitos de arquitetura tecnológica descritos a seguir:

4.16.1. Recursos de prevenção contra ameaças avançadas em tempo real (IPS, antivírus e proteção contra zero-day).

4.16.2. Ferramentas de controle de aplicações e filtragem de conteúdo para evitar acessos a sites ou serviços indevidos.

4.16.3. Alta disponibilidade, com redundância de hardware para garantir a continuidade dos serviços.

4.16.4. Compatibilidade nativa com o software de gerenciamento Palo Alto Panorama atualmente utilizado pelo IFRN.

Requisitos de Projeto e de Implementação

4.17. Os equipamentos deverão observar integralmente os requisitos de projeto e de implementação descritos nas tabelas contidas no Subitem 3.4 "DESCRIÇÃO DETALHADA DA SOLUÇÃO DE TIC" deste Termo de Referência.

Requisitos de Implantação

4.18. Os equipamentos deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

4.18.1. A implantação deverá ser realizada por profissionais especializados da contratada, que possuam certificação do fabricante da solução adquirida que lhes confirmam as competências necessárias para a realização dos respectivos serviços de implantação, ou pelo próprio fabricante.

4.18.2. Deverá abranger a configuração de quaisquer funcionalidades suportadas pelos equipamentos / softwares. Estas informações serão documentadas no termo de abertura do projeto a ser elaborado pela CONTRATADA após alinhamento do escopo de trabalho definido entre CONTRATADA e CONTRATANTE.

Requisitos de Garantia, Manutenção e Assistência Técnica

4.19. O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, **60 (sessenta) meses**, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

4.20. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem

qualquer ônus ou custo adicional para o Contratante.

4.21. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

4.22. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

4.23. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

4.24. Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até **05 (cinco) dias úteis**, contados a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.

4.25. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.

4.26. Na hipótese do subitem acima, o Contratado deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

4.27. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

4.28. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.

4.29. A garantia legal ou contratual do objeto tem prazo de vigência própria e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

4.30. Os chamados poderão ser abertos ou diretamente com o fabricante ou com a autorizada oficial do fabricante no Brasil durante a vigência da garantia.

4.31. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs.

Requisitos de Experiência Profissional

4.32. Os serviços de instalação e configuração dos itens relacionados neste termo de referência deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, com certificação oficial do fabricante, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

4.33. A contratada deverá possuir, no mínimo, um técnico certificado oficialmente pelo fabricante da solução.

4.34. Não serão exigidos requisitos de formação da equipe para a presente contratação.

Requisitos de Metodologia de Trabalho

4.35. O fornecimento dos equipamentos está condicionado ao recebimento pelo Contratado de Ordem de fornecimento de Bens (OFB) emitida pela Contratante.

4.36. A OFB indicará o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.

4.37. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento **24 horas por dia e 7 dias por semana** de maneira eletrônica e **8 horas por dia e 5 dias por semana** por via telefônica.

4.38. O andamento do fornecimento dos equipamentos deve ser acompanhado pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

Requisitos de Segurança da Informação e Privacidade

4.39. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

4.39.1. A Contratada deverá manter a integridade da rede de dados e das informações do IFRN durante a prestação dos serviços.

4.39.2. A Contratada deverá respeitar a Política de Segurança da Informação e Comunicações do IFRN bem como demais políticas e normas internas que poderão ser instituídas durante a vigência do contrato. A Contratada deverá guardar sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

4.39.3. Qualquer unidade de armazenamento, tais como SSDs, HDDs e memórias, utilizadas deverão permanecer em posse da Contratante mesmo após o uso, após dano à unidade ou após o término do contrato. Caso seja necessária a remoção de alguma unidade de armazenamento, esta ação deverá ser realizada no prédio do IFRN e imediatamente entregue a Contratante.

4.39.4. Caso haja necessidade de manutenção fora das dependências do IFRN, as unidades de armazenamento deverão ser removidas dentro das dependências do IFRN e deverão ficar sob responsabilidade da Contratante enquanto perdurar o conserto.

Outros Requisitos Aplicáveis

Sustentabilidade

4.40. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.40.1. Bens constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448- 1 e 15448-2;

4.40.2. Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

4.40.3. Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenilpolibromados (PBDEs).

Indicação de marcas ou modelos:

4.41. Na presente contratação será admitida a indicação da(s) seguinte(s) marca(s), característica(s) ou modelo(s), de acordo com as justificativas contidas nos Estudos Técnicos Preliminares:

4.41.1. Soluções de Firewall de Próxima Geração da Palo Alto Networks.

Subcontratação

4.42. Não será admitida a subcontratação do objeto contratual.

4.43. A vedação à subcontratação decorre da natureza integrada e crítica da solução de segurança cibernética objeto da contratação, que envolve fornecimento de equipamentos, licenciamento, suporte técnico especializado, garantia do fabricante, implantação e integração à infraestrutura institucional de TIC do IFRN. A execução do objeto exige responsabilidade técnica centralizada, atuação coordenada e domínio integral da solução ofertada, de modo a assegurar a interoperabilidade entre os componentes, a continuidade operacional dos serviços institucionais e a adequada prestação da garantia e do suporte técnico durante toda a vigência contratual. A subcontratação poderia dificultar a definição de responsabilidades, comprometer a rastreabilidade das atividades executadas e aumentar os riscos relacionados à segurança da informação e à disponibilidade da infraestrutura tecnológica institucional. Adicionalmente, verifica-se a existência de empresas no mercado com capacidade técnica e operacional para executar integralmente o objeto, não havendo prejuízo à competitividade do certame.

Garantia da contratação

- 4.43. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, podendo o Contratado optar pela caução em dinheiro ou em títulos da dívida pública, seguro-garantia, fiança bancária ou título de capitalização, em valor correspondente a **5% (cinco por cento)** do valor **total** da contratação.
- 4.44. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.
- 4.44.1. A apólice de seguro-garantia permanecerá em vigor mesmo que o Contratado não pague o prêmio nas datas convencionadas.
- 4.44.2. Caso o adjudicatário não apresente a apólice de seguro de garantia antes da assinatura do contrato, ocorrerá a preclusão do direito de escolha dessa modalidade de garantia.
- 4.44.3. A apólice de seguro-garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.
- 4.44.4. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvados os períodos de suspensão contratual.
- 4.44.5. Caso o adjudicatário não opte pelo seguro-garantia ou não apresente a apólice de seguro de garantia antes da assinatura do contrato, deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contado da assinatura do contrato, comprovante de prestação de garantia nas modalidades de caução em dinheiro ou títulos da dívida pública, fiança bancária ou títulos de capitalização.
- 4.45. Caso seja a garantia em dinheiro a modalidade de garantia escolhida pelo Contratado, deverá ser efetuada em favor do Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.[A30]
- 4.46. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério competente.
- 4.47. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.
- 4.48. Na hipótese de opção pelo título de capitalização, a garantia deverá ser custeada por pagamento único, com resgate pelo valor total, sob a modalidade de instrumento de garantia, emitido por sociedades de capitalização regulamente constituídas e autorizadas pelo Governo Federal.
- 4.48.1. O título de capitalização deverá ser apresentado ao Contratante juntamente com as condições gerais e o número do processo administrativo sob o qual o plano de capitalização foi aprovado pela Susep (art. 8º, III, da Circular SUSEP nº 656, de 11 de março de 2022).
- 4.49. A garantia assegurará, qualquer que seja a modalidade escolhida, sob pena de não aceitação, o pagamento de:
- 4.49.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas; e
- 4.49.2. multas moratórias e punitivas aplicadas pela Administração ao Contratado.
- 4.50. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, contado da data de assinatura do termo aditivo ou da emissão do apostilamento, seguindo os mesmos parâmetros utilizados quando da contratação.
- 4.51. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o Contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

4.52. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contados da data em que for notificada[A31] .

4.53. O Contratante executará a garantia na forma prevista na legislação que rege a matéria.

4.53.1. O emitente da garantia ofertada pelo Contratado deverá ser notificado pelo Contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

4.53.2. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.

4.54. Extinguir-se-á a garantia com a restituição da carta fiança, autorização para a liberação de importâncias depositadas em dinheiro a título de garantia ou anuência ao resgate do título de capitalização, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que o Contratado cumpriu todas as cláusulas do contrato.

4.54.1. A extinção da garantia na modalidade seguro-garantia observará a regulamentação da Susep.

4.54.2. A Administração deverá apurar se há alguma pendência contratual antes do término da vigência da apólice.

4.55. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

4.56. O Contratado autoriza o Contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Termo de Referência.

4.57. O garantidor não é parte para figurar em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções ao Contratado.

4.58. A garantia de execução é independente de eventual garantia do produto ou serviço prevista neste Termo de Referência.

Informações relevantes para a apresentação da proposta

4.59. A proposta deve observar o § 4º do art. 12 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, que preconiza que nas licitações por preço global, cada serviço ou produto do lote deverá estar discriminado em itens separados nas propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB, de acordo com o art. 26 da Lei nº 14.133, de 2021.

Reserva de cotas para microempresas e empresas de pequeno porte:

4.60. Não serão aplicadas as reservas de cotas de até 25% para microempresas e empresas de pequeno porte, conforme facultado pelo Art. 49, inciso II, da Lei Complementar nº 123/2006, pelos seguintes motivos técnicos e operacionais:

4.60.1. Risco de Inexecução: A solução demandada exige alta robustez financeira para a manutenção de estoques de reposição e cumprimento de prazos. A reserva de cotas para ME/EPP poderia comprometer a rede do IFRN caso a contratada não possua capilaridade logística ou capacidade financeira para suportar as garantias e substituições de hardware em tempo hábil, caracterizando o prejuízo à execução do objeto.

4.60.2. Prejuízo ao conjunto e à padronização: A solução de Firewall de Próxima Geração (NGFW) exige que os novos ativos operem sob a mesma arquitetura lógica e sistema operacional do parque tecnológico já estabelecido no IFRN. A fragmentação do lote entre fornecedores ou marcas distintas comprometeria a formação de túneis VPN estáveis, a sincronização de políticas de segurança e a inteligência compartilhada de ameaças.

4.60.2. Gerenciamento centralizado: O IFRN utiliza gestão centralizada para resposta a incidentes. A coexistência de soluções heterogêneas (marcas diferentes) inviabilizaria a aplicação de políticas globais de segurança em tempo real, aumentando a vulnerabilidade da rede e os custos operacionais de manutenção e treinamento.

4.60.3. Economia de escala e unicidade de suporte: O agrupamento em lote único visa atrair fornecedores aptos a entregar a solução integrada ao ecossistema atual do IFRN, garantindo melhores preços por escala e, principalmente, um canal unificado de suporte técnico e atualização de assinaturas de segurança, em observância ao Princípio da Eficiência (Art. 5º da Lei nº 14.133/2021).

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3. receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável; e

5.1.8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.2. São obrigações do CONTRATADO:

5.2.1. indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do contrato;

5.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.3. reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do contrato pela Contratante;

5.2.4. propiciar todos os meios necessários à fiscalização do contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

- 5.2.5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- 5.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- 5.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;
- 5.2.8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração; e
- 5.2.9. fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso.

5.3. São obrigações do órgão gerenciador do registro de preços:

- 5.3.1. efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;
- 5.3.2. conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;
- 5.3.3. definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:
- 5.3.3.1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e
- 5.3.3.2. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;
- 5.3.4. definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:
- 5.3.4.1. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;
- 5.3.4.2. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo Contratado; e
- 5.3.4.3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 deste artigo, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

6. MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de Execução

Do Encaminhamento Formal de Demandas

- 6.1. O gestor do contrato emitirá a Ordem de fornecimento de bens (OFB) para a entrega dos bens desejados.
- 6.2. O Contratado deverá fornecer equipamentos com as mesmas configurações e quantidades definidas na OFB.
- 6.3. O recebimento provisório e definitivo dos bens é disciplinado em tópico próprio deste TR.
- 6.3.1. Os bens serão recebidos provisoriamente, quando da entrega integral do objeto (incluindo todas as parcelas), pelo (a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.
- 6.3.2. Os bens serão recebidos definitivamente no prazo de 10 (dez) dias úteis, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo

circunstanciado desde que estejam de acordo com os critérios de aceitação constante neste Termo de Referência.

Forma de execução e acompanhamento do contrato

Condições de Entrega

6.4. O prazo de entrega dos bens é de **120** dias, contados do **recebimento da Ordem de Fornecimento de Bens (OFB)**, em remessa única.

6.5. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos **10** dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

6.6. Os bens deverão ser entregues no seguinte endereço: IFRN - REITORIA, Rua Dr. Nilo Bezerra Ramalho, nº 1692, Tirol. Natal/RN. CEP: 59015-300. Telefone: (84) 4005-0890. E-mail: ditic@ifrn.edu.br

Formas de transferência de conhecimento

6.7. Não será necessária transferência de conhecimento devido às características do objeto.

Procedimentos de transição e finalização do contrato

6.8. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

Quantidade mínima de bens ou serviços para comparação e controle

6.9. Cada OFB conterà a quantidade a ser fornecida, incluindo a sua localização e o prazo, conforme definições deste TR.

Mecanismos formais de comunicação

6.10. São definidos como mecanismos formais de Comunicação, entre a Contratante e o Contratado, os seguintes:

- I) Ordem de Fornecimento de Bens;
- II) Ata de Reunião;
- III) Ofício;
- IV) Sistema de abertura de chamados;
- V) E-mails e Cartas.

Formas de Pagamento

6.11. Os critérios de medição e pagamento serão tratados em tópico próprio do Modelo de Gestão do Contrato.

Manutenção de Sigilo e Normas de Segurança

6.12. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução do contrato, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.13. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos ANEXOS: Anexo - Modelo de Termo de Compromisso e Manutenção de Sigilo.

7. MODELO DE GESTÃO DO CONTRATO

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Reunião Inicial

7.5. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução do contrato.

7.6. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até **10** dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.7. A pauta desta reunião observará, pelo menos:

7.7.1. Presença do representante legal da contratada, que apresentará o seu preposto;

7.7.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

7.7.3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.7.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

7.7.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

Fiscalização

7.8. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

7.9. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.10. O fiscal técnico do contrato anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

7.11. Identificada qualquer inexecução ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.12. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.13. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

7.14. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

Fiscalização Administrativa

7.15. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.16. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

7.17. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da Contratante ou de seus agentes, gestores e fiscais, de conformidade.

Gestor do Contrato

7.18. Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:

7.18.1. . coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

7.18.2. acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

7.18.3. acompanhar a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

7.18.4. emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

7.18.5. tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

7.18.6. elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

7.18.7. enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7.19. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual.

Critérios de Aceitação

- 7.20. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:
- 7.21. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não reconicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).
- 7.22. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.
- 7.23. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.
- 7.24. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.
- 7.25. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.
- 7.26. Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.
- 7.27. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões “shareware” ou “trial”. O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.
- 7.28. A Contratante poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade.
- 7.29. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.
- 7.30. Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital. Em caso de dúvida ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em dias úteis após a solicitação até 15 (quinze) deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnico certificado na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão (conforme itens 1.1.1 e 1.1.2, TC-006.806/2006-4, Acórdão nº 838/2006-TCU-2ª Câmara.

Procedimentos de Teste e Inspeção

7.31. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

- 7.31.1. Previamente ao recebimento definitivo da solução serão realizados a verificação, testes e inspeção do atendimento integral às especificações técnicas exigidas. Estas ações serão realizadas por equipe designada pelo Coordenador de Tecnologia da Informação acompanhados dos fiscais do contrato.
- 7.31.2. Inicialmente deverá ser realizada a verificação das especificações exigidas através da inspeção física dos equipamentos, análise dos manuais técnicos enviados juntamente com os equipamentos ou disponibilizados de alguma forma e da análise de informações disponibilizadas no site da fabricante. Para esta etapa deve-se observar a seguinte lista de verificação:
- 7.31.3. Verificar se a caixa do equipamento foi entregue lacrada, em embalagem original e apresentando identificações de marca e modelo de acordo a descrição da proposta da CONTRATADA;
- 7.31.4. Verificar se o equipamento está novo e sem uso;
- 7.31.5. Verificar se o equipamento é o mesmo equipamento que foi ofertado na proposta;
- 7.31.6. Verificar se o equipamento foi entregue acompanhado de todos os acessórios previstos nas especificações técnicas (como cabo de energia, conectores, etc.) e descritos na documentação apresentada junto com a proposta da CONTRATADA;
- 7.31.7. Verificar se o(s) equipamentos(s) foram entregues na(s) quantidade(s) correta(s);
- 7.31.8. Verificar se a documentação mínima exigida foi entregue (exceto relatório de implantação);
- 7.31.9. Verificar se os equipamentos foram recebidos de forma que funcionem na tensão elétrica entre 120 à 240 V.

Níveis Mínimos de Serviço Exigidos

7.32. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAE – INDICADOR DE ATRASO NO FORNECIMENTO DO EQUIPAMENTO		
Tópico	Descrição	
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens.	
Meta a cumprir	IAE < = 0	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento de Bens dentro do prazo previsto.
Instrumento de medição	OFB, Termo de Recebimento Provisório (TRP)	
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OFB. Será subtraída a data de entrega dos produtos da OFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OFB.	
Periodicidade	Para cada Ordem de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.	

Mecanismo de Cálculo (métrica)	IAE = <u>TEX – TEST</u> Onde: IAE – Indicador de Atraso de Entrega da OFB; TEX – Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB. A data de início será aquela constante na OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB. A data de entrega da OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OFB continua a correr, findando-se apenas quanto o Contratado entrega os produtos da OFB e haja aceitação por parte do fiscal técnico. TEST – Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência.
Observações	Obs1: Serão utilizados dias corridos na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.
Início de Vigência	A partir da emissão da OFB.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IAE: Menor ou igual a 0 – Pagamento integral da OFB; De 1 a 60 - aplicar-se-á glosa de 0,1666% por dia de atraso sobre o valor da OFB ou fração em atraso. Acima de 60 - aplicar-se-á glosa de 10% bem como multa de 2% sobre o valor OFB ou fração em atraso.

8. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NOS PAGAMENTOS

8.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
		Multa de 0,5% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por

1	Não prestar os esclarecimentos imediatamente, referente à execução do contrato, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de (48) horas úteis.	escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 5 (cinco) dias úteis.
		Após o limite de 5 (cinco) dias úteis, aplicar-se-á multa de 0,75% do valor total do Contrato.
2	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OS)	Glosa de 0,5% sobre o valor da OS para valores do indicador IAE de 0,11 a 0,20.
		Glosa de 0,5% sobre o valor da OS para valores do indicador IAE de 0,21 a 0,30.
		Glosa de 0,5% sobre o valor da OS para valores do indicador IAE de 0,31 a 0,50.
		Glosa de 0,5% sobre o valor da OS para valores do indicador IAE de 0,51 a 1,00.
		Multa de 0,5% sobre o valor do Contrato e Glosa de 0,5% sobre o valor da OS, para valores do indicador IAE maiores que 1,00.
3	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência.
		Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 0,5% do valor total do Contrato.

8.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o Contratado:

8.2.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

8.2.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

8.3. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

8.4. Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

8.4.1 Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

8.4.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

8.4.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

8.4.4. Multa:

8.4.4.1. Moratória, para as infrações descritas no item “d”, de **0,5% (cinco décimos por cento)** por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de **30 (trinta)** dias;

8.4.4.2. Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia;

8.4.4.2.1. O atraso superior a 25 (vinte e cinco) dias para apresentação, suplementação ou reposição da garantia autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

8.4.4.3. Compensatória, para as infrações descritas acima alíneas “e” a “h” de **1,0% (um por cento) a 15% (quinze por cento)** do valor da contratação.

8.4.4.4. Compensatória, para a inexecução total do contrato prevista acima na alínea “c”, de **20% (vinte por cento) a 30% (trinta por cento)** do valor da contratação.

8.4.4.5. Compensatória, para a infração descrita acima na alínea “b”, de **5,0% (cinco por cento) a 15% (quinze por cento)** do valor da contratação.

8.4.4.6. Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de **2,0% (dois por cento) a 10% (dez por cento)** do valor da contratação.

8.4.4.7. Compensatória, para a infração descrita acima na alínea “a”, de **5,0% (cinco por cento) a 15% (quinze por cento)** do valor da contratação.

8.5. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

8.6. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

8.7. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

8.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

8.9. A multa poderá ser recolhida administrativamente no prazo máximo de **30 (trinta)** dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.10. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

8.10.1. Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

8.10.2. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no SICAF serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

8.11. Na aplicação das sanções serão considerados:

8.11.1. a natureza e a gravidade da infração cometida;

8.11.2. as peculiaridades do caso concreto;

8.11.3. as circunstâncias agravantes ou atenuantes;

8.11.4. os danos que dela provierem para o Contratante; e

8.11.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

8.12. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

8.13. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

8.14. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

8.14.1. As penalidades serão obrigatoriamente registradas no SICAF.

8.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

8.16. Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do Objeto

9.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

9.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de **30 (trinta)** dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

9.3. O recebimento definitivo ocorrerá no prazo de **10 (dez)** dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

9.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até **5 (cinco)** dias úteis.

9.5. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

9.6. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

9.7. O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

9.8. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens nem a responsabilidade ético-profissional pela perfeita execução do contrato.

9.9. As atividades de montagem, instalação e quaisquer outras necessárias para o funcionamento ou uso do bem correrão por conta do Contratado e são condição para o recebimento do objeto.

Liquidação

9.10. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.

9.11. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

9.12. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

9.12.1. o prazo de validade;

9.12.2. a data da emissão;

9.12.3. os dados do contrato e do órgão contratante;

9.12.4. o período respectivo de execução do contrato;

9.12.5. o valor a pagar; e

9.12.6. eventual destaque do valor de retenções tributárias cabíveis.

9.13. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante;

9.14. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

9.15. A Administração deverá realizar consulta ao SICAF para:

9.15.1. verificar a manutenção das condições de habilitação exigidas;

9.15.2. identificar possível razão que impeça a participação em licitação/contratação no âmbito do órgão ou entidade, tais como a proibição de contratar com a Administração ou com o Poder Público, bem como ocorrências impeditivas indiretas.

9.16. Constatando-se, junto ao SICAF, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

9.17. Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

9.18. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

9.19. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o Contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

9.20. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

9.21. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do **Índice de Custo da Tecnologia da Informação (ICTI)** de correção monetária.

Forma de pagamento

9.22. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

9.23. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

9.24. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

9.25. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

9.26. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Cessão de Crédito

9.27. As cessões de crédito dependerão de prévia aprovação do Contratante.

9.27.1. A eficácia da cessão de crédito, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

9.27.2. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.

9.27.3. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta

vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

9.27.4. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do Contratado.

9.28. O disposto nesta seção não afeta as operações de crédito de que trata a Instrução Normativa SEGES/MGI nº 82, de 21 de fevereiro de 2025, as quais ficam por esta regidas.

Reajuste

9.29. Os preços inicialmente contratados são fixos e irredutíveis no prazo de um ano contado da data do orçamento estimado, em 13 de maio de 2026.

9.30. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI[A19] , mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

9.31. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

9.32. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

9.33. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

9.34. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

9.35. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

9.36. O reajuste será realizado por apostilamento.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

Forma de seleção e critério de julgamento da proposta

10.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

Forma de fornecimento

10.2. O fornecimento do objeto será parcelado. O fornecimento dos bens e a implantação da solução ocorrerão de forma parcelada, mediante emissão de ordens de fornecimento pela Administração, conforme cronograma de execução a ser definido pelo IFRN, observadas as necessidades operacionais dos campi e dos ambientes de datacenter. As contratações decorrentes da Ata de Registro de Preços serão realizadas de forma gradual, de acordo com a disponibilidade orçamentária, o planejamento institucional e as prioridades definidas pela área de Tecnologia da Informação e Comunicação. A Administração poderá emitir ordens de fornecimento e implantação por etapas, observando critérios relacionados à continuidade operacional da infraestrutura institucional de TIC, à disponibilidade orçamentária, ao planejamento da migração tecnológica, à maturidade dos ambientes de implantação e à priorização das unidades institucionais.

Critérios de aceitabilidade de preços

10.3. Em se tratando de contratação para Registro de Preços, com critério de julgamento pelo menor preço do grupo, a aceitabilidade da proposta será aferida com base no valor global do grupo e nos preços unitários máximos admitidos para cada item que o compõe.

10.3.1. Os preços unitários máximos aceitáveis corresponderão aos valores constantes da planilha de formação de preços que integra o processo administrativo e servirão como limite para fins de julgamento da proposta.

Exigências de habilitação

10.4. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos:

Habilitação jurídica

10.5. pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

10.6. empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.7. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

10.8. sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

10.9. sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

10.10. sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.11. filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

10.12. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

10.13. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

10.14. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta n.º 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

10.15. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

10.16. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei n.º 5.452, de 1º de maio de 1943;

- 10.17. Prova de inscrição no cadastro de contribuintes Estadual ou Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- 10.18. Prova de regularidade com a Fazenda Estadual ou Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
- 10.19. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.
- 10.20. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

- 10.21. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua participação na licitação/contratação, ou de sociedade simples;
- 10.22. certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;
- 10.23. balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos dois últimos exercícios sociais, já exigíveis e apresentados na forma da lei, comprovando, índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da aplicação das seguintes fórmulas[A10] :

LG =

Ativo Circulante + Realizável a Longo Prazo

Passivo Circulante + Passivo Não Circulante

SG =

Ativo Total

Passivo Circulante + Passivo Não Circulante

LC =

Ativo Circulante

Passivo Circulante

- 10.24. Caso a empresa interessada apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de até 10% do valor total estimado da contratação.
- 10.25. Os indicadores fixados acima deverão ser atingidos em cada um dos dois últimos exercícios sociais, sob pena de inabilitação;
- 10.26. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;
- 10.27. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

10.28. As empresas criadas no exercício financeiro da licitação/contratação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

10.29. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

Qualificação Técnica

10.30. Deve ser apresentado atestado de capacidade técnica comprovando que a licitante é apta a fornecer, instalar e configurar as soluções referentes a este termo de referência. A Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, se dará por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

10.30.1. Para fins da comprovação de que trata o subitem 10.33, o(s) atestado(s) deverá(ão) demonstrar que a licitante executou satisfatoriamente contrato(s) envolvendo solução de segurança de rede de complexidade tecnológica e operacional equivalente ou superior à desta contratação, contemplando, no mínimo:

10.30.1.1. fornecimento de equipamentos de firewall de próxima geração (Next Generation Firewall – NGFW), ou solução de segurança de rede de natureza e complexidade tecnológica equivalentes;

10.30.1.2. execução de serviços de instalação, configuração e implantação dos equipamentos ou da solução de segurança de rede fornecida; e

10.30.1.3. integração da solução implantada a ambiente corporativo de Tecnologia da Informação e Comunicação – TIC.

10.30.2. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

10.30.3. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da Contratante e local em que foi executado o objeto Contratado, dentre outros documentos.

10.31. A contratada deverá possuir, pelo menos, um técnico certificado pelo fabricante compatível com o objeto deste termo de referência;

10.31.1. A comprovação de vínculo profissional se fará com a apresentação de cópia da carteira de trabalho (CTPS) em que conste o licitante como contratante; do contrato social do licitante em que conste o profissional como sócio; do contrato de prestação de serviços, sem vínculo trabalhista, regido pela legislação civil ou, ainda, de declaração de contratação futura do profissional, desde que acompanhada de declaração de anuência do profissional.

Disposições gerais sobre habilitação

10.32. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

10.33. Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou da ata de registro de preços ou do aceite do instrumento equivalente, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

10.34. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

10.35. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.36. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação, que corresponde ao valor máximo aceitável, é de **R\$ 4.364.122,70 (quatro milhões e trezentos e sessenta e quatro mil e cento e vinte e dois reais e setenta centavos)**, conforme custos unitários apostos na **tabela contida no item 1.1 acima**.

11.2. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre Contratante e Contratado, conforme especificado na matriz de risco constante do Contrato.

11.3. Em caso de Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

- 11.3.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;
- 11.3.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;
- 11.3.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou
- 11.3.4. poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

12.2. A contratação será atendida pela seguinte dotação:

- I) Gestão/unidade:-;
- II) Fonte de recursos: -;
- III) Programa de trabalho: -;
- IV) Elemento de despesa: -; e
- V) Plano interno:-

12.3. *A indicação da dotação orçamentária fica postergada para o momento da assinatura do contrato ou instrumento equivalente.*

13. DISPOSIÇÕES FINAIS

13.1. As informações contidas neste Termo de Referência não são classificadas como sigilosas.

--	--	--

Integrante Requisitante <u>João Rodrigo Silva de Carvalho</u> <u>Técnico de Tecnologia da</u> <u>Informação</u> <u>Mat. 1877397</u>	Integrante Técnico <u>Alex Augusto de Souza Santos</u> <u>Tecnico de Laboratorio Area -</u> <u>Manutenção e Suporte de</u> <u>Computadores</u> <u>Mat. 1928999</u>	Integrante Administrativo <u>Francisca Simonely de</u> <u>Vasconcelos</u> <u>Administrador</u> <u>Mat. 2087066</u>
---	---	--

Autoridade Máxima da Área de TIC
Tarso Latorraca Casadei <u>Diretor Sistêmico de Tecnologia da Informação e Comunicação</u> <u>Mat. 1878646</u>

Natal, 24 de agosto de 2026.

Aprovo,

Autoridade Competente
Roberto Gomes Cavalcante Junior <u>Pró-Reitor de Administração em Exercício</u> <u>Mat. 1730348</u>

14. 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 10:00:20.

FRANCISCA SIMONELY DE VASCONCELOS

Membro da comissão de contratação



Assinou eletronicamente em 24/08/2026 às 09:45:58.

Despacho: Aprovo o presente Termo de Referência, atestando sua conformidade técnica e autorizando o prosseguimento da contratação, nos termos da IN SGD nº 94/2022.

TARSO LATORRACA CASADEI

Autoridade Máxima da Área de TIC



Assinou eletronicamente em 24/08/2026 às 09:56:50.

Despacho: Aprovo o Termo de Referência, considerando a relevância, necessidade, adequação dos recursos e resultados esperados, conforme fundamentado nos autos.

ROBERTO GOMES CAVALCANTE JUNIOR

Autoridade competente



Assinou eletronicamente em 24/08/2026 às 10:39:18.

Documento Digitalizado Público

TR158155_000133_2026

Assunto: TR158155_000133_2026
Assinado por: Simonely Vasconcelos
Tipo do Documento: Termo de Referência
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 11:18:56.

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: 2698698
Código de Autenticação: 8cd370ab8c

