



Proposta Comercial

Registro de Preços – SRP, para o fornecimento de solução tecnológica de Controlador de Entrega de Aplicações (*Application Delivery Controller – ADC*), incluindo os serviços de instalação, configuração, suporte técnico mensal e transferência de conhecimento, bem como serviços técnicos especializados, sob demanda, para implementação e customização da solução, com vistas a atender às necessidades do Conselho da Justiça Federal e demais órgãos partícipes.

Pregão Eletrônico N° 90008/2025

Brasília, 19 de agosto de 2025.

Prezado(a), **CONSELHO DA JUSTIÇA FEDERAL.**

Aos cuidados da **Seção de Licitações.**

Setor de Clubes Esportivos Sul – SCES, Trecho III, Polo 8, Lote 9,
CEP: 70.200-003, Brasília/DF.

PROPOSTA DE PREÇOS – NEGOCIADA

Referência: **PREGÃO ELETRÔNICO Nº 90008/2025**
Processo Administrativo nº: 0000919-34.2024.4.90.8000

LAYER TECNOLOGIA DA INFORMAÇÃO LTDA, inscrita no CNPJ nº 04.929.322/0001-70 e inscrição estadual nº 07.632.255/001-78, estabelecida na SHN QUADRA 1 CONJUNTO A BLOCO A ENTRADA A, SALAS 708/709, Asa Norte, Cep 70.701-010 – Brasília/DF, apresenta, proposta comercial para Registro de Preços para fornecimento de solução tecnológica de Controlador de Entrega de Aplicações (*Application Delivery Controller* – ADC), incluindo os serviços de instalação, configuração, suporte técnico mensal e transferência de conhecimento, bem como serviços técnicos especializados, sob demanda, para implementação e customização da solução, com vistas a atender às necessidades do Conselho da Justiça Federal e demais órgãos partícipes, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

Atenciosamente,

**VICTOR
ARAUJO
FREIRE:533410
82115**

Digitally signed by
VICTOR ARAUJO
FREIRE:53341082115
Date: 2025.08.19
21:28:27 -03'00'

VICTOR ARAUJO FREIRE
Responsável Legal

Assinado de forma digital por RODRIGO GARCIA
MEDEIROS:28404795835
DN: c=BR, o=ICP-Brasil, ou=Secretaria da Receita Federal do Brasil
- RFB, ou=RFB e-CPF A1, ou=(EM BRANCO), ou=24398727000137,
ou=videoconferencia, cn=RODRIGO GARCIA
MEDEIROS:28404795835
Dados: 2025.08.20 10:03:18 -03'00'

RODRIGO GARCIA MEDEIROS
Responsável Legal

LAYER TECNOLOGIA DA INFORMAÇÃO LTDA

1 Sobre a Layer

Na Layer acreditamos que a chave para o sucesso no ambiente digital está em **conectar o presente e proteger o futuro**. Oferecemos soluções avançadas em infraestrutura de dados e cibersegurança que permitem às empresas não apenas otimizar sua operação no agora, mas também se proteger contra os desafios e ameaças do amanhã.

Nossa expertise em **infraestrutura de dados** garante que sua empresa tenha uma base sólida e escalável, capaz de armazenar, processar e gerenciar grandes volumes de informações com eficiência. Ao integrar essa infraestrutura com soluções de **cibersegurança** de ponta, oferecemos uma proteção contínua contra as ameaças digitais, assegurando a confidencialidade, integridade e disponibilidade dos dados.

Combinando inovação, tecnologia de ponta e conhecimento especializado, nossa missão é fornecer um ambiente seguro, resiliente e preparado para o futuro, permitindo que nossos clientes se concentrem no crescimento do seu negócio com total confiança na sua infraestrutura de dados.

2 Programa de Integridade

O programa de integridade Layer, é uma iniciativa que busca promover uma cultura de ética, transparência e conformidade nas operações da empresa. Ele envolve a implementação de políticas e procedimentos que visam prevenir e detectar comportamentos ilegais, antiéticos e fraudes, tanto por parte dos colaboradores quanto dos fornecedores e parceiros de negócios.

Além disso, nosso programa de integridade contempla a realização periódica de treinamentos, bem como contemplou a criação de canais de denúncia e a realização de auditorias regulares para garantir que as políticas estão sendo seguidas e a cultura de integridade está sendo mantida. A implementação do programa de integridade trouxe diversos benefícios para a empresa, como o fortalecimento da reputação, a redução de riscos legais e a melhoria do desempenho financeiro. Nosso programa de integridade está disponível em https://layer.net.br/wp-content/uploads/2023/10/Layer_Programa-de-Integridade-.pdf.



A Layer conquistou ainda em 2021 o selo CertiGov

. O selo ajuda a manter o fomento de uma cultura ética de anticorrupção e antissuborno na empresa, fornecedores e parceiros, de forma que tenham o mesmo rigor com padrões éticos e normas anticorrupção em que se baseiam. O selo trouxe os seguintes benefícios a empresa:

- Fortalecimento da cultura e práticas de antissuborno e anticorrupção por toda a empresa.
- Redução do risco do envolvimento em situações ilícitas e fraudulentas.
- Melhoria da governança empresarial.
- Aumento da credibilidade junto a clientes do setor público e privado.
- Manutenção da prática de compliance de forma preventiva e não reativa.
- Garantia de eficiência e aumento de segurança nas práticas de vendas para o mercado.

3 Proposta de Preços

GP	ITEM	DESCRIÇÃO	UNIDADE	QTD.	VALOR UNITÁRIO	VALOR TOTAL
1	1.1	Appliance físico para solução de Application Delivery Controller – ADC, fabricante F5, Modelo BIG-IP R4800	Und	10	1.790.000,00	17.900.000,00
	1.2	Serviço de instalação e configuração da solução ADC	Und	10	88.000,00	880.000,00
	1.3	Serviço de garantia e suporte técnico presencial para a solução ADC	Mês	300	13.000,00	3.900.000,00
	1.4	Transferência de conhecimento online, com carga horária mínima de 40h	Pessoa	20	25.000,00	500.000,00
	1.5	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	2960	275,00	814.000,00
2	2.1	Appliance virtual para solução ADC, Tipo 1, incluindo licenciamento/subscrições para 60 (sessenta) meses	Und	8	450.000,00	3.600.000,00
	2.2	Appliance virtual para solução ADC, Tipo 2, incluindo licenciamento/subscrições para 60 (sessenta) meses	Und	6	890.000,00	5.340.000,00
	2.3	Serviço de instalação e configuração da solução ADC	Und	14	45.000,00	630.000,00
	2.4	Serviço de suporte técnico remoto para a solução ADC	Mês	84	18.000,00	1.512.000,00
	2.5	Transferência de conhecimento online, com carga horária mínima de 40h	Pessoa	21	25.000,00	525.000,00
	2.6	Serviços técnicos especializados para implementação e customização da solução ADC	Hora	1400	275,00	385.000,00
					Valor Total G1	23.994.000,00
					Valor Total G2	11.992.000,00
					Valor Total	35.986.000,00

3.1 Valores da Proposta:

3.1.1 Grupo 01: **R\$ 23.994.000,00** (vinte e três milhões, novecentos e noventa e quatro mil reais)

3.1.2 Grupo 02: **R\$ 11.992.000,00** (onze milhões, novecentos e noventa e dois mil reais)

3.1.3 Total: **R\$ 35.986.000,00** (trinta e cinco milhões, novecentos e oitenta e seis mil reais).

3.2 A proposta é válida por 90 (noventa) dias, a contar da data de sua apresentação.

3.3 O detalhamento da marca, modelo, versão e demais características dos produtos e serviços ofertados constam da **Seção Caderno Técnico**.

4 Dados da Empresa

Dados da empresa			
Razão Social: LAYER TECNOLOGIA DA INFORMAÇÃO LTDA			
CNPJ: 04.929.322/0001-70		Inscrição Estadual nº: 07.632.255/001-78	
Endereço: SHN QUADRA 1 CONJUNTO A BLOCO A ENTRADA A, SALAS 708/709, Asa Norte			
Telefone: (61) 3544-7273		Fax: (61) 3544-7273	
E-mail: comercial@layer.net.br		Cidade/UF: Brasília/DF	Cep: 70.701.010
Representantes legais com poderes para assinar o contrato <u>CONJUNTAMENTE</u>			
Nome	Cargo	e-mail	
Rodrigo Garcia Medeiros	Diretor Comercial	comercial@layer.net.br	
Victor Araújo Freire	Diretor Executivo	comercial@layer.net.br	
Dados Para Suporte			
Telefone: 61-3544-7273	e-mail: suporte@layer.net.br	site suporte: https://layer.movidesk.com/	

5 Declarações

Layer Tecnologia da Informação Ltda, através dos seus representantes legais, declara para os devidos fins que se aplicam a presente proposta que:

- 5.1 está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;
- 5.2 não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição.

- 5.3 não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal.
- 5.4 cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.
- 5.5 não se enquadra como Microempresa ou empresa de pequeno porte, e atesta que não irá usufruir do tratamento favorecido estabelecido nos arts. 42 a 49 da Lei Complementar Federal nº. 123/06.
- 5.6 nos preços apresentados, já estão computados todos os custos necessários decorrentes do fornecimento de produtos e da prestação dos serviços, bem como já incluídos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais, e quaisquer outros que incidam direta ou indiretamente na execução do objeto.
- 5.7 Os bens ofertados atendem aos critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos no art. 3º, II, do Decreto nº 7.174, de 12 de maio de 2010 e pela Portaria INMETRO nº 170, de 10 de abril de 2012.
- 5.8 cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório.
- 5.9 a empresa optou pela **não realização da vistoria técnica** nas instalações físicas do **CONSELHO DA JUSTIÇA FEDERAL**, tendo ciência que não poderá alegar em qualquer fase da licitação ou vigência da relação contratual que não realizará os serviços em conformidade com a qualidade e requisitos exigidos e que tem pleno conhecimento das condições e peculiaridades inerentes à natureza do trabalho, assume total responsabilidade por este fato e não utilizará deste para quaisquer questionamentos futuros que ensejem desavenças técnicas ou financeiras com a contratante.
- 5.10 inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores.
- 5.11 tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.
- 5.12 temos pleno conhecimento das condições necessárias para prestação dos serviços.
- 5.13 está garantida a exequibilidade da proposta comercial apresentada, assegurando que os preços e condições ofertados refletem a viabilidade técnica e econômica para a execução completa dos serviços/produtos especificados no edital. A proposta considera todos os requisitos exigidos, garantindo a qualidade, os prazos, os recursos e o atendimento às normas legais e regulatórias aplicáveis, visando ao pleno cumprimento do objeto contratado e à satisfação dos critérios de eficiência e economicidade estabelecidos.
- 5.14 para todos os fins e efeitos legais, aceitar, irrestritamente, todas as condições e exigências estabelecidas no Edital da licitação em referência e do Contrato a ser celebrado, cuja minuta constitui Anexo do Edital.
- 5.15 inexistente qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista com servidores ou dirigente do **CJF**.
- 5.16 Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

- 5.17 nos valores propostos estão inclusas todas as despesas, inclusive frete, tributos e encargos de qualquer natureza incidentes sobre o objeto do Edital, nada mais sendo lícito pleitear a esse título.
- 5.18 estamos de pleno acordo com as condições estabelecidas no Edital e seus anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas nos documentos de contratação.
- 5.19 a proposta foi elaborada de forma independente.
- 5.20 sob as penas da Lei nº 6.938/1981, na qualidade de proponente do procedimento licitatório, sob a modalidade Pregão Eletrônico Nº **90008/2025**, que atendemos aos critérios de qualidade ambiental e sustentabilidade socioambiental, respeitando as normas de proteção do meio ambiente.
- 5.21 estamos cientes da obrigatoriedade da apresentação das declarações e certidões pertinentes dos órgãos competentes quando solicitadas como requisito para habilitação e da obrigatoriedade do cumprimento integral ao que estabelece o art. 6º e seus incisos, da Instrução Normativa nº 01, de 19 de janeiro de 2010.
- 5.22 a signatária não se encontra suspensa de licitar ou contratar com o **CJF**.
- 5.23 a produtividade adotada é a utilizada pela Administração como referência.
- 5.24 além do escopo de fornecimento proposto, não há outros materiais e equipamentos que serão utilizados na execução dos serviços.
- 5.25 executaremos o contrato e os serviços de acordo com as especificações e condições estabelecidas no Edital e seus Anexos.
- 5.26 em caso de ausência ou divergência entre qualquer declaração aqui expressa com as requisitadas no Edital e seus Anexos, atesta que está ciente e de acordo com as expressas no Edital e seus anexos.

6 Escopo de Fornecimento

6.1 Fabricantes e Fornecedores

Fornecedor	País	Nome do Representante	E-mail	Telefone	Site
Layer Tecnologia	Brasil	Victor Araújo Freire Rodrigo Garcia Medeiros	comercial@layer.net.br	(61) 3544-7273	https://www.layer.net.br
FF Network	USA	Tiago Silva	t.dasilva@f5.com	61) 99649-4787	https://www.f5.com

6.2 Composição

6.2.1 Grupo 1

ITEM	DESCRIÇÃO			UND.	QTD ITEM
1.1	Appliance físico para solução de Application Delivery Controller – ADC, fabricante F5, Modelo BIG-IP R4800			Unidade	10
	Fornecedor: F5	Produto/Serviço: F5-BIG-LTM-R4600	Versão: n/a		
Subitem	Código	Descrição			Qtd. Total
1	F5-BIG-LTM-R4600	SOLUTION CONSISTS OF: 1X F5-BIG-LTM-R4600, 1X extra F5-UPG-AC-R4XXX, 4X F5-UPG-SFP+-R Obs1: As interfaces ópticas de 10GE podem ser substituídas por 25GE a critério do CJF. Obs2: cada interface contempla cordão óptico LC/LC duplex OM4 multimodo 2,5 metros.			10
2	F5-ADD-BIG-GBT-R48XX	BIG-IP Local Traffic Manager to Best Bundle Upgrade for r4800			10
3	F5-SBS-BIG-TC-1-1YR	BIG-IP Threat Campaigns License for r4X00 r2X00 i4X00 i2X00 Advanced Web Application Firewall 1-Year Subscription			20
4	F5-ADD-BIG-R46R48	BIG-IP r4600 to r4800 License Upgrade			10
5	F5-SBS-BIG-TC-1-3YR	BIG-IP Threat Campaigns License for r4X00 r2X00 i4X00 i2X00 Advanced Web Application Firewall 3-Year Subscription			10
6	F5-SBS-BIG-IPI-4-1YR	BIG-IP IP Intelligence License for r4X00 i4X00 1-Year Subscription			20
7	F5-SBS-BIG-IPI-4-3YR	BIG-IP IP Intelligence License for r4X00 i4X00 3-Year Subscription			10
8	F5-SVC-BIG-PRE-HW364	BIG-IP SERVICE PREMIUM CAT HW364			50
9	F5-SVC-BIG-PRE-SW210	BIG-IP Service Premium CAT SW210			50
10	F5-SVC-BIG-PRE-SW209	BIG-IP Service Premium CAT SW209			50

ITEM	DESCRIÇÃO			UND.	QTD ITEM
1.2	Serviço de instalação e configuração da solução ADC			Unidade	10
	Fornecedor: Layer	Produto/Serviço: Serviços de Instalação de ADC	Versão: n/a		
Subitem	Descrição				Qtd. Total
1	Serviços Layer	Serviços de Instalação de ADC			10

ITEM	DESCRIÇÃO			UND.	QTD ITEM
1.3	Serviço de garantia e suporte técnico presencial para a solução ADC			Mês	300
	Fornecedor: Layer	Produto/Serviço: Serviços de Suporte Mensal de ADC	Versão: n/a		
Subitem	Descrição				Qtd. Total
1	Serviços Layer	Serviços de Suporte Mensal de ADC			300

ITEM	DESCRIÇÃO			UND.	QTD ITEM
1.4	Transferência de conhecimento online, com carga horária mínima de 40h			Pessoa	20
	Fornecedor: Layer	Produto/Serviço:	Versão: n/a		
Subitem	Descrição				Qtd. Total
1	Serviços Layer	Serviço de transferência de conhecimento			20

ITEM	DESCRIÇÃO			UND.	QTD ITEM
1.5	Serviços técnicos especializados para implementação e customização da solução ADC			Hora	2.960
	Fornecedor: Layer	Produto/Serviço: Serviços técnicos especializados	Versão: n/a		
Subitem	Descrição				Qtd. Total
1	Serviços Layer	Serviços técnicos especializados para implementação e customização da solução ADC			2.960

6.2.2 Grupo 2

ITEM	DESCRIÇÃO			UND.	QTD ITEM
2.1	Appliance virtual para solução ADC, Tipo 1, incluindo licenciamento/subscrições para 60 (sessenta) meses			Unidade	08
	Fornecedor: F5	Produto/Serviço: F5-BIG-VE-BT-1G-V23	Versão: n/a		
Subitem	Descrição				Qtd. Total
1	F5-BIG-VE-BT-1G-V23		BIGIP VIRTUAL EDITION: BEST BUNDLE 1 GBPS (V17.1.X - V23.X)		8
2	F5-SVC-BIG-PRE-SW531		BIG-IP Service Premium CAT SW531		40
3	F5-SBS-BIGVE-IP121YR		BIG-IP Virtual Edition IP Intelligence License 1-Year Subscription 1 Gbps 3 Gbps and 5 Gbps		16
4	F5-SBS-BIGVE-IP123YR		BIG-IP Virtual Edition IP Intelligence License 3-Year Subscription 1 Gbps 3 Gbps and 5 Gbps		8
5	F5-SBS-BIG-VE-TC21YR		BIG-IP Virtual Edition Threat Campaigns Add-on License for Advanced Web Application Firewall 1 Gbps 1-Year Subscription		16
6	F5-SBS-BIG-VE-TC23YR		BIG-IP Virtual Edition Threat Campaigns Add-on License for Advanced Web Application Firewall 1 Gbps 3-Year Subscription		8

ITEM	DESCRIÇÃO			UND.	QTD ITEM
2.2	Appliance virtual para solução ADC, Tipo 2, incluindo licenciamento/subscrições para 60 (sessenta) meses			Unidade	06
	Fornecedor: F5	Produto/Serviço: F5-BIG-VE-BT-10G-V23	Versão: n/a		
Subitem	Descrição				Qtd. Total
1	F5-BIG-VE-BT-10G-V23	BIG-IP VIRTUAL EDITION BEST BUNDLE 10 GBPS (V171X - V23X)			6
2	F5-SVC-BIG-PRE-SW561	BIG-IP Service Premium CAT SW561			30
3	F5-SBS-BIGVE-IP131YR	BIG-IP Virtual Edition IP Intelligence License 1-Year Subscription 10 Gbps			12
4	F5-SBS-BIGVE-IP133YR	BIG-IP Virtual Edition IP Intelligence License 3-Year Subscription 10 Gbps			6
5	F5-SBS-BIG-VE-TC31YR	BIG-IP Virtual Edition Threat Campaigns Add-on License for Advanced Web Application Firewall 3 Gbps and High Performance 1-Year Subscription			12
6	F5-SBS-BIG-VE-TC33YR	BIG-IP Virtual Edition Threat Campaigns Add-on License for Advanced Web Application Firewall 3 Gbps and High Performance 3-Year Subscription			6

ITEM	DESCRIÇÃO			UND.	QTD ITEM
2.3	Serviço de instalação e configuração da solução ADC			Unidade	14
	Fornecedor: Layer	Produto/Serviço: Serviços de Instalação de ADC	Versão: n/a		
Subitem	Descrição				Qtd. Total
1	Serviços Layer	Serviços de Instalação de ADC			14

ITEM	DESCRIÇÃO			UND.	QTD ITEM
2.4	Serviço de suporte técnico remoto para a solução ADC			Mês	84
	Fornecedor: Layer	Produto/Serviço: Serviços de Suporte Mensal de ADC	Versão: n/a		
Subitem	Descrição				Qtd. Total
1	Serviços Layer	Serviços de Suporte Mensal de ADC			84

ITEM	DESCRIÇÃO			UND.	QTD ITEM
2.5	Transferência de conhecimento online, com carga horária mínima de 40h			Pessoa	21
	Fornecedor: Layer	Produto/Serviço:	Versão: n/a		
Subitem	Descrição				Qtd. Total
1	Serviços Layer	Serviço de transferência de conhecimento			21

ITEM	DESCRIÇÃO			UND.	QTD ITEM
2.6	Serviços técnicos especializados para implementação e customização da solução ADC			Hora	1.400
	Fornecedor: Layer	Produto/Serviço:	Versão: n/a		
Subitem	Descrição				Qtd. Total
1	Serviços Layer	Serviços técnicos especializados para implementação e customização da solução ADC			1.400

7 Descrição

7.1 ITEM 1.1 - Appliance físico para solução de Application Delivery Controller – ADC, fabricante F5, Modelo BIG-IP R4800.

7.1.1 Visão Geral



O F5 BIG-IP R4800 é um appliance físico de ADC que integra hardware especializado com o software BIG-IP, oferecendo uma solução completa para balanceamento de carga, segurança de aplicações e otimização de performance. Esta solução foi projetada para atender organizações que necessitam de alta disponibilidade, performance excepcional e segurança avançada para suas aplicações críticas de negócio.

7.1.2 Sobre o Hardware

O appliance de ADC modelo **F5 R4800** é uma plataforma de hardware de última geração que oferece uma arquitetura altamente escalável baseada em microsserviços para potencializar suas aplicações essenciais para a missão e implantações de rede. Esses dispositivos de alto desempenho incluem FPGAs modernos para possibilitar um descarregamento de SSL, além de possibilitar a utilização de algoritmos de curva elíptica (ECC). Com um poderoso desempenho de L7 request-per-second (RPS), o rSeries permite consolidar vários serviços em um único dispositivo e aumenta a densidade de portas de alta velocidade por unidade de rack.



O **F5 R4800** oferece o nível incomparável de desempenho e proteção que suas aplicações essenciais e implantações de rede exigem. Projetado em uma nova camada de plataforma baseada em microsserviços, o rSeries possibilita a consolidação, reduzindo os custos e o TCO em toda a infraestrutura

Uma nova revolução no design da plataforma rSeries equilibram desempenho, escalabilidade e segurança, permitindo que a TI descarregue três vezes mais no geral o processamento de SSL e implemente entrega de aplicações e serviços de segurança abrangentes em qualquer lugar

- **Proteja aplicações com criptografia** — Criptografia líder do setor e aceleração de hardware de codificações ECC.

- **Escale o processamento de descarregamento de SSL** — O melhor desempenho de SSL do mercado acelera a adoção de SSL/TLS ao descarregar o oneroso processamento de SSL e aumenta a velocidade de troca de chaves e criptografia em massa.
- **Mitigue vetores de ameaças** — Reduza os riscos com proteção de mais de 100 vetores de ataque, como denial-of-service (DoS) e ataques DDoS, com detecção e mitigação.



7.1.3 Sobre o Software

O **software BIG-IP** que opera no R4800 representa mais de vinte e cinco anos de inovação em sistemas operacionais especializados para entrega de aplicações. Este sistema foi desenvolvido especificamente para otimizar o processamento de tráfego de rede, oferecendo capacidades avançadas que não são encontradas em sistemas operacionais convencionais.

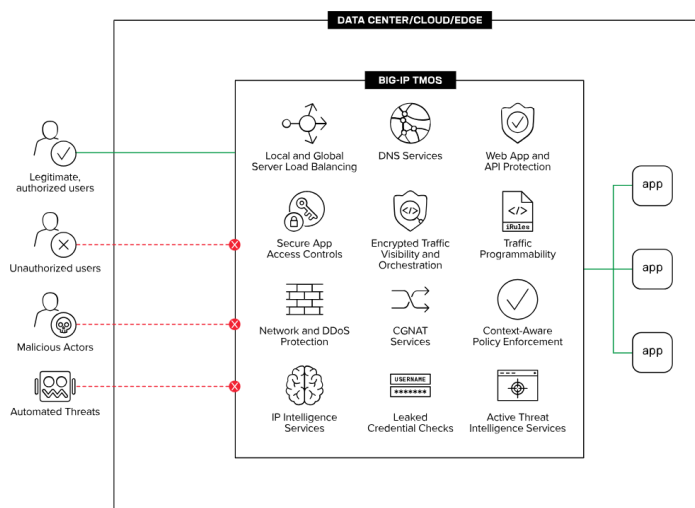


Figura 1 - Arquitetura BIG-IP

O licenciamento ofertado é o **BEST BUNDLE**, composto pelos seguintes módulos: **LTM, DNS, APM, AFM e Advanced WAF(antigo ASM)**. Ainda estão inclusos neste item os serviços de subscrição **IP Intelligence e Threat Campaigns** para um período de 60 meses.



O sistema de balanceamento de carga do BIG-IP vai muito além de simples distribuição de tráfego, implementando algoritmos inteligentes que consideram múltiplos fatores como carga do servidor, tempo de resposta, localização geográfica e conteúdo da requisição para tomar decisões de roteamento otimizadas. mente o tráfego entre servidores em um data center, enquanto o balanceamento de carga global estende essas capacidades através de múltiplos data centers e regiões geográficas.

As funcionalidades de segurança incluem um Web Application Firewall de classe enterprise que protege contra vulnerabilidades OWASP Top 10, ataques de injeção SQL, cross-site scripting e muitas outras técnicas de ataque. A proteção de APIs oferece capacidades especializadas para ambientes de microserviços, incluindo validação de esquemas, rate limiting inteligente e proteção contra ataques específicos de APIs.



O sistema implementa proteção DDoS multicamada que opera tanto em nível de rede quanto de aplicação. A proteção de rede utiliza técnicas de rate limiting e análise de padrões de tráfego para identificar e mitigar ataques volumétricos, enquanto a proteção de aplicação analisa o comportamento de requisições individuais para detectar ataques mais sofisticados.

O componente de Access Policy Manager (APM) oferece funcionalidades avançadas de controle de acesso e autenticação, permitindo implementar políticas granulares de segurança baseadas em identidade, dispositivo, localização e contexto. O APM suporta múltiplos métodos de autenticação incluindo autenticação multifator, integração com diretórios corporativos como Active Directory e LDAP, e federação de identidades através de protocolos como SAML e OAuth.

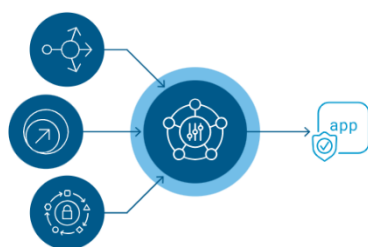


Já o módulo DNS do BIG-IP proporciona serviços DNS de alta performance e disponibilidade, oferecendo capacidades que vão desde resolução DNS básica até funcionalidades avançadas de balanceamento de carga global e proteção contra ataques DNS. O sistema pode atuar como servidor DNS autoritativo, resolver recursivo ou proxy DNS, suportando grandes volumes de consultas com baixa latência. As funcionalidades incluem DNS caching inteligente, proteção contra ataques de amplificação DNS, rate limiting por origem, e integração com sistemas de inteligência de ameaças para bloqueio automático de domínios maliciosos. O módulo também oferece capacidades de Global Server Load Balancing (GSLB), permitindo distribuição inteligente de tráfego entre múltiplos data centers baseadas em critérios como proximidade geográfica, saúde dos servidores e políticas de negócio, garantindo que usuários sejam sempre direcionados para o recurso mais apropriado e disponível.

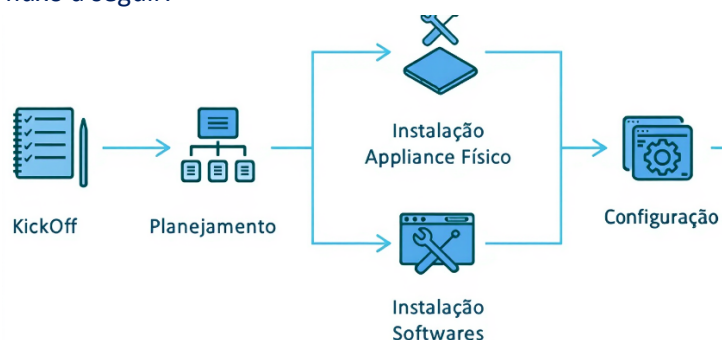
O BIG-IP oferece extensas capacidades de programabilidade através do sistema iRules, que permite a criação de lógica customizada para processamento de tráfego utilizando uma linguagem de script que oferece acesso a todos os aspectos de uma conexão de rede. Para ambientes modernos de DevOps, o sistema oferece APIs RESTful abrangentes que permitem integração com ferramentas de orquestração e automação completa de tarefas de configuração e manutenção.



7.2 ITEM 1.2 - Serviço de instalação e configuração da solução ADC.



Os **serviços de instalação, configuração da solução de ADC** sempre realizados em plena conformidade com os requisitos do Edital e seus Anexos, independente da descrição aqui realizada. O processo de instalação é efetuado com segurança pelo nosso time de consultores especializados, de forma faseada conforme o fluxo a seguir:



- **Kickoff:**
 - Contempla a apresentação de equipes, escopo de projeto e fases da implantação e definição de pontos focais.
- **Planejamento:**
 - De acordo com a necessidade do projeto, é desenhada a melhor abordagem para o processo de instalação, configuração e disponibilização da solução em produção. Além das estratégias, são definidas questões de arquitetura, plano operacional da instalação e requisitos.
- **Instalação Física:**
 - Remoção dos equipamentos das caixas;
 - Instalação física nos racks;
 - Conectorização dos cabos de rede e de energia;
 - Organização de cabos;
 - Configuração IPs de gerenciamento;
 - Testes de conectividade;
 - Monitoramento;
 - Testes de redundância de fontes;
 - Testes preliminares de alta disponibilidade de caixa.
- **Instalação de Softwares:**
 - Instalação de softwares nos equipamentos.
 - Configurações Básicas de rede;
 - Ativação de Licenças;
 - Testes;
 - Monitoramento.
- **Configuração Lógica:**

- Configuração inicial conforme recomendação do fabricante e seguindo as orientações da CONTRATANTE, contemplando no mínimo as atividades no Edital, bem como demais funcionalidades relacionadas ao ambiente;
- **Documentação:**
 - Documentação completa e detalhada do projeto como construído (as-built), constando, minimamente, as configurações efetuadas, topologia, usuários e senhas inicialmente configurados.
- **Certificação do Ambiente:**
 - Após a configuração completa do ambiente, é iniciado um processo de teste completo para certificar que todas as configurações e integrações estão operantes.
- **Ativação do Ambiente:**
 - Uma vez certificado, o ambiente é ativado em produção e está preparado para início da operação.

7.3 ITEM 1.3 - Serviço de garantia e suporte técnico presencial para a solução ADC.



Os serviços serão sempre realizados em plena conformidade com os requisitos do edital e seus Anexos, **independente da descrição aqui realizada.**

Durante a vigência contratual a Layer Tecnologia realizará a prestação de serviços suporte técnico pelo período de 60 (sessenta) meses abrangendo no mínimo os aspectos listados nas páginas 42 a 44 do TR.

7.4 ITEM 1.4 - Transferência de conhecimento online, com carga horária mínima de 40h.



Os serviços serão sempre realizados em plena conformidade com os requisitos do edital e seus Anexos, **independente da descrição aqui realizada.** A transferência de conhecimentos provida abordará todos os componentes da solução fornecida, e ainda estará de acordo com a utilização da solução instalada no ambiente da CONTRATANTE, abrangendo no mínimo os tópicos listados nas páginas 44 a 45 do TR.

7.5 ITEM 1.5 - Serviços técnicos especializados para implementação e customização da solução ADC



Os serviços serão sempre realizados em plena conformidade com os requisitos do edital e seus Anexos, **independente da descrição aqui realizada.**

Os Serviços técnicos especializados para implementação e customização da solução ADC são compostos por um conjunto de atividades que permita a implementação de novas funcionalidades e readequações do ambiente, bem

como o aprimoramento do conhecimento da equipe técnica da CONTRATANTE responsável pelas atividades de administração e operação da solução. Os serviços devem abranger no mínimo os aspectos listados nas páginas 46 a 48 do TR.

7.6 ITEM 2.1 - Appliance virtual para solução ADC, Tipo 1, incluindo licenciamento/subscrições para 60 (sessenta) meses.

7.6.1 Visão Geral



O **F5 BIG-IP Virtual Edition (VE)** é uma versão virtual do sistema BIG-IP que opera como uma máquina virtual, oferecendo os mesmos serviços de um hardware dedicado. O BIG-IP VE é um controlador de entrega de aplicativos (ADC) virtual que oferece serviços avançados de tráfego, segurança e aceleração de aplicações. Ele é compatível com os principais hipervisores e plataformas de nuvem, como VMware vSphere, Microsoft Hyper-V, Google Cloud e Amazon Web Services. A plataforma permite a automação e orquestração dos serviços, integrando-se a ferramentas de CI/CD como Ansible, Jenkins e Terraform.

7.6.2 Capacidade de Throughput Licenciada

O Appliance virtual de ADC Tipo 1 possui uma capacidade licenciada **de 1 Gbps**.

7.6.3 Sobre o Software

O software BIG-IP que opera no **appliance virtual Tipo 1** representa mais de vinte e cinco anos de inovação em sistemas operacionais especializados para entrega de aplicações. Este sistema foi desenvolvido especificamente para otimizar o processamento de tráfego de rede, oferecendo capacidades avançadas que não são encontradas em sistemas operacionais convencionais.

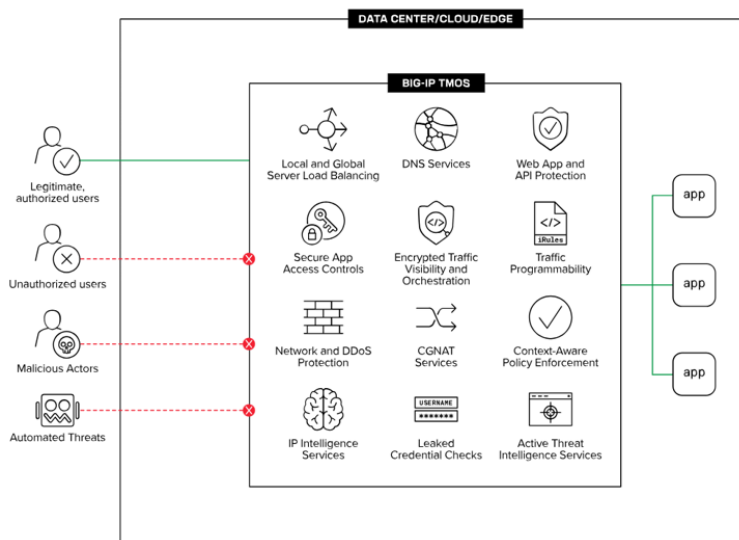


Figura 2 - Arquitetura BIG-IP

O licenciamento ofertado é o **BEST BUNDLE**, composto pelos seguintes módulos: **LTM, DNS, APM, AFM e Advanced WAF(antigo ASM)**. Ainda estão inclusos neste item os serviços de subscrição **IP Intelligence e Threat Campaigns** para um período de 60 meses.



O sistema de balanceamento de carga do BIG-IP vai muito além de simples distribuição de tráfego, implementando algoritmos inteligentes que consideram múltiplos fatores como carga do servidor, tempo de resposta, localização geográfica e conteúdo da requisição para tomar decisões de roteamento otimizadas. mente o tráfego entre servidores em um data center, enquanto o balanceamento de carga global estende essas capacidades através de múltiplos data centers e regiões geográficas.

As funcionalidades de segurança incluem um Web Application Firewall de classe empresarial que protege contra vulnerabilidades OWASP Top 10, ataques de injeção SQL, cross-site scripting e muitas outras técnicas de ataque. A proteção de APIs oferece capacidades especializadas para ambientes de microserviços, incluindo validação de esquemas, rate limiting inteligente e proteção contra ataques específicos de APIs.



O sistema implementa proteção DDoS multicamada que opera tanto em nível de rede quanto de aplicação. A proteção de rede utiliza técnicas de rate limiting e análise de padrões de tráfego para identificar e mitigar ataques volumétricos, enquanto a proteção de aplicação analisa o comportamento de requisições individuais para detectar ataques mais sofisticados.

O componente de Access Policy Manager (APM) oferece funcionalidades avançadas de controle de acesso e autenticação, permitindo implementar políticas granulares de segurança baseadas em identidade, dispositivo, localização e contexto. O APM suporta múltiplos métodos de autenticação incluindo autenticação multifator, integração com diretórios corporativos como Active Directory e LDAP, e federação de identidades através de protocolos como SAML e OAuth.



Já o módulo DNS do BIG-IP proporciona serviços DNS de alta performance e disponibilidade, oferecendo capacidades que vão desde resolução DNS básica até funcionalidades avançadas de balanceamento de carga global e proteção contra ataques DNS. O sistema pode atuar como servidor DNS autoritativo, resolver recursivo ou proxy DNS, suportando grandes volumes de consultas com baixa latência. As funcionalidades incluem DNS caching inteligente, proteção contra ataques de amplificação DNS, rate limiting por origem, e integração com sistemas de inteligência de ameaças para bloqueio automático de domínios maliciosos. O módulo também oferece capacidades de Global Server Load Balancing (GSLB), permitindo distribuição inteligente de tráfego entre múltiplos data centers baseadas em critérios como proximidade geográfica, saúde dos servidores e políticas de negócio, garantindo que usuários sejam sempre direcionados para o recurso mais apropriado e disponível.

O BIG-IP oferece extensas capacidades de programabilidade através do sistema iRules, que permite a criação de lógica customizada para processamento de tráfego utilizando uma linguagem de script que oferece acesso a todos os aspectos de uma conexão de rede. Para ambientes modernos de DevOps, o sistema oferece APIs RESTful abrangentes que permitem integração com ferramentas de orquestração e automação completa de tarefas de configuração e manutenção.



7.7 ITEM 2.2 - Appliance virtual para solução ADC, Tipo 2, incluindo licenciamento/subscrições para 60 (sessenta) meses.

7.7.1 Visão Geral



O **F5 BIG-IP Virtual Edition (VE)** é uma versão virtual do sistema BIG-IP que opera como uma máquina virtual, oferecendo os mesmos serviços de um hardware dedicado. O BIG-IP VE é um controlador de entrega de aplicativos (ADC) virtual que oferece serviços avançados de tráfego, segurança e aceleração de aplicações. Ele é compatível com os principais hipervisores e plataformas de nuvem, como VMware vSphere, Microsoft Hyper-V, Google Cloud e Amazon Web Services. A plataforma permite a automação e orquestração dos serviços, integrando-se a ferramentas de CI/CD como Ansible, Jenkins e Terraform.

7.7.2 Capacidade de Throughput Licenciada

O Appliance virtual de ADC Tipo 2 possui uma capacidade licenciada **de 10 Gbps**.

7.7.3 Sobre o Software

O software BIG-IP que opera no **appliance virtual Tipo 2** representa mais de vinte e cinco anos de inovação em sistemas operacionais especializados para entrega de aplicações. Este sistema foi desenvolvido especificamente para otimizar o processamento de tráfego de rede, oferecendo capacidades avançadas que não são encontradas em sistemas operacionais convencionais.

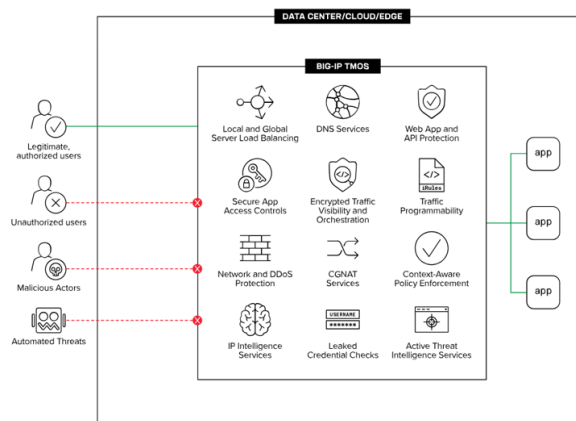


Figura 3 - Arquitetura BIG-IP

O licenciamento ofertado é o **BEST BUNDLE**, composto pelos seguintes módulos: **LTM, DNS, APM, AFM e Advanced WAF(antigo ASM)**. Ainda estão inclusos neste item os serviços de subscrição **IP Intelligence e Threat Campaigns** para um período de 60 meses.



O sistema de balanceamento de carga do BIG-IP vai muito além de simples distribuição de tráfego, implementando algoritmos inteligentes que consideram múltiplos fatores como carga do servidor, tempo de resposta, localização geográfica e conteúdo da requisição para tomar decisões de roteamento otimizadas. mente o tráfego entre servidores em um data center, enquanto o balanceamento de carga global estende essas capacidades através de múltiplos data centers e regiões geográficas.

As funcionalidades de segurança incluem um Web Application Firewall de classe empresarial que protege contra vulnerabilidades OWASP Top 10, ataques de injeção SQL, cross-site scripting e muitas outras técnicas de ataque. A proteção de APIs oferece capacidades especializadas para ambientes de microserviços, incluindo validação de esquemas, rate limiting inteligente e proteção contra ataques específicos de APIs.



O sistema implementa proteção DDoS multicamada que opera tanto em nível de rede quanto de aplicação. A proteção de rede utiliza técnicas de rate limiting e análise de padrões de tráfego para identificar e mitigar ataques volumétricos, enquanto a proteção de aplicação analisa o comportamento de requisições individuais para detectar ataques mais sofisticados.

O componente de Access Policy Manager (APM) oferece funcionalidades avançadas de controle de acesso e autenticação, permitindo implementar políticas granulares de segurança baseadas em identidade, dispositivo, localização e contexto. O APM suporta múltiplos métodos de autenticação incluindo autenticação multifator, integração com diretórios corporativos como Active Directory e LDAP, e federação de identidades através de protocolos como SAML e OAuth.

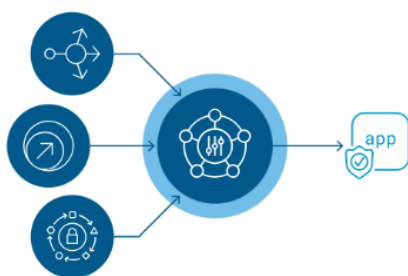


Já o módulo DNS do BIG-IP proporciona serviços DNS de alta performance e disponibilidade, oferecendo capacidades que vão desde resolução DNS básica até funcionalidades avançadas de balanceamento de carga global e proteção contra ataques DNS. O sistema pode atuar como servidor DNS autoritativo, resolver recursivo ou proxy DNS, suportando grandes volumes de consultas com baixa latência. As funcionalidades incluem DNS caching inteligente, proteção contra ataques de amplificação DNS, rate limiting por origem, e integração com sistemas de inteligência de ameaças para bloqueio automático de domínios maliciosos. O módulo também oferece capacidades de Global Server Load Balancing (GSLB), permitindo distribuição inteligente de tráfego entre múltiplos data centers baseadas em critérios como proximidade geográfica, saúde dos servidores e políticas de negócio, garantindo que usuários sejam sempre direcionados para o recurso mais apropriado e disponível.

O BIG-IP oferece extensas capacidades de programabilidade através do sistema iRules, que permite a criação de lógica customizada para processamento de tráfego utilizando uma linguagem de script que oferece acesso a todos os aspectos de uma conexão de rede. Para ambientes modernos de DevOps, o sistema oferece APIs RESTful abrangentes que permitem integração com ferramentas de orquestração e automação completa de tarefas de configuração e manutenção.

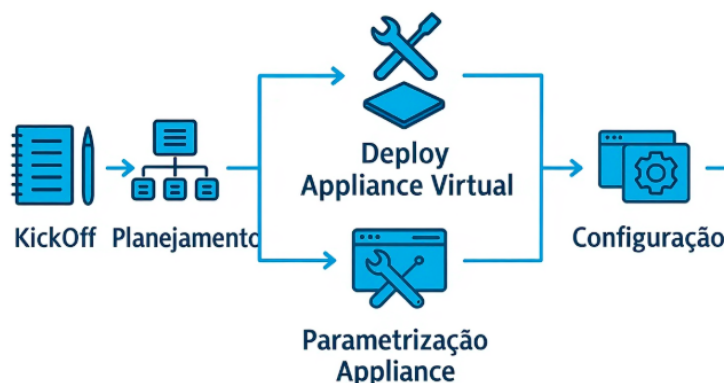


7.8 ITEM 2.3 - Serviço de instalação e configuração da solução ADC.



Os **serviços de instalação, configuração da solução de ADC** sempre realizados em plena conformidade com os requisitos do Edital e seus Anexos, independente da descrição aqui realizada.

O processo de instalação é efetuado com segurança pelo nosso time de consultores especializados, de forma faseada conforme o fluxo a seguir:



- **Kickoff:**
 - Contempla a apresentação de equipes, escopo de projeto e fases da implantação e definição de pontos focais.
- **Planejamento:**
 - De acordo com a necessidade do projeto, é desenhada a melhor abordagem para o processo de instalação, configuração e disponibilização da solução em produção. Além das estratégias, são definidas questões de arquitetura, plano operacional da instalação e requisitos.
- **Instalação de Softwares:**
 - Instalação de softwares nos equipamentos.
 - Configurações Básicas de rede;
 - Ativação de Licenças;
 - Testes;
 - Monitoramento.

- **Configuração Lógica:**
 - Configuração inicial conforme recomendação do fabricante e seguindo as orientações da CONTRATANTE, contemplando no mínimo as atividades no Edital, bem como demais funcionalidades relacionadas ao ambiente;
- **Documentação:**
 - Documentação completa e detalhada do projeto como construído (as-built), constando, minimamente, as configurações efetuadas, topologia, usuários e senhas inicialmente configurados.
- **Certificação do Ambiente:**
 - Após a configuração completa do ambiente, é iniciado um processo de teste completo para certificar que todas as configurações e integrações estão operantes.
- **Ativação do Ambiente:**
 - Uma vez certificado, o ambiente é ativado em produção e está preparado para início da operação.

7.9 ITEM 2.4 - Serviço de suporte técnico remoto para a solução ADC



Os serviços serão sempre realizados em plena conformidade com os requisitos do edital e seus Anexos, **independente da descrição aqui realizada.**

Durante a vigência contratual a Layer Tecnologia realizará a prestação de serviços suporte técnico pelo período de 12 (doze) meses abrangendo no mínimo os aspectos listados nas páginas 42 a 44 do TR.

7.10 ITEM 2.5 - Transferência de conhecimento online, com carga horária mínima de 40h.



Os serviços serão sempre realizados em plena conformidade com os requisitos do edital e seus Anexos, **independente da descrição aqui realizada.** A transferência de conhecimentos provida abordará todos os componentes da solução fornecida, e ainda estará de acordo com a utilização da solução instalada no ambiente da CONTRATANTE, abrangendo no mínimo os tópicos listados nas páginas 44 a 47 do TR.

7.11 ITEM 2.6 - Serviços técnicos especializados para implementação e customização da solução ADC.



Os serviços serão sempre realizados em plena conformidade com os requisitos do edital e seus Anexos, **independente da descrição aqui realizada.**

Os Serviços técnicos especializados para implementação e customização da solução ADC são compostos por um conjunto de atividades que permita a implementação de novas funcionalidades e readequações do ambiente, bem como o aprimoramento do conhecimento da equipe técnica da CONTRATANTE

responsável pelas atividades de administração e operação da solução. Os serviços devem abranger no mínimo os aspectos listados nas páginas 46 a 48 do TR.

8 Comprovações Técnicas

- 8.1 Nesta seção estão comprovados os requisitos mínimos e obrigatórios para os itens do escopo de fornecimento.
- 8.2 Consta anexo à presente proposta, documentação técnica (manuais, catálogos oficiais do fabricante, links URL etc.) que comprova o pleno atendimento a todos os requisitos técnicos listados no **“ANEXO I e II – DETALHAMENTO DOS REQUISITOS TÉCNICOS”** do Termo de Referência, através de planilha ponto a ponto, com indicação de nome do documento e página que comprovam o atendimento.
- 8.3 Estamos cientes que a CONTRATANTE poderá a qualquer momento realizar diligência junto a licitante e/ou fabricante para comprovação da veracidade de qualquer documento apresentado.
- 8.4 Os seguintes documentos são partes integrantes da presente proposta:
 - 8.4.1 000-Comprovacao-Ponto-a-Ponto-v4.pdf
 - 8.4.2 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf
 - 8.4.3 011-ANATEL-Certificado-de-homologacao.pdf
 - 8.4.4 012-F5-hardware-product-lifecycle-support-policy.pdf
 - 8.4.5 013-F5-plataform-overview.pdf
 - 8.4.6 014-F5-Platform-Specifications.pdf
 - 8.4.7 015-F5-rSeries-High-Availability.pdf
 - 8.4.8 016-F5-Network-Settings.pdf
 - 8.4.9 017-F5-Creating-an-Active-Active-Configuration-using-the-Configuration-Utility.pdf
 - 8.4.10 030-F5-Download-products-from-MyF5.pdf
 - 8.4.11 040-F5-System-Settings.pdf
 - 8.4.12 050-F5-User-Management.pdf
 - 8.4.13 060-F5-System-Overview.pdf
 - 8.4.14 070-F5-Additional-System-Tasks.pdf
 - 8.4.15 080-F5-iControlREST-Home.pdf
 - 8.4.16 090-F5-icontrol-rest-api-user-guide-16-1-0.pdf
 - 8.4.17 100-F5-Load-Balancing-to-IPv6-Nodes.pdf
 - 8.4.18 110-F5-Services-Profiles.pdf
 - 8.4.19 120-F5-On-Demand-Certificate-Authentication.pdf
 - 8.4.20 130-F5-LDAP Query.pdf
 - 8.4.21 140-F5-Preventing-TCP-Connection-Requests-From-Being-Dropped.pdf

- 8.4.22 150-F5-packet-filtering.pdf
- 8.4.23 160-F5-About-AFM-DoS_DDoS-Protection.pdf
- 8.4.24 170-F5-Remove-Server-Header-Information-in-HTTP-Responses.pdf
- 8.4.25 180-F5-Log-files-and-alerts.pdf
- 8.4.26 190-F5-About-Logging.pdf
- 8.4.27 200-F5-Web-Acceleration.pdf
- 8.4.28 210-F5-Container-Ingress-Services.pdf
- 8.4.29 220-F5-Service-Type-LoadBalancer.pdf
- 8.4.30 221-F5-Virtual-Server.pdf
- 8.4.31 222-F5-reverse-proxy-server.pdf
- 8.4.32 223-F5-SSL-Methods-for-LTM.pdf
- 8.4.33 224-F5-Maximum-number-of-members-allowed-in-a pool.pdf
- 8.4.34 225-F5-LTM-load-balancing.pdf
- 8.4.35 226-F5-Persistence-methods.pdf
- 8.4.36 227-F5-Compression.pdf
- 8.4.37 228-F5-OneConnect-profile.pdf
- 8.4.38 229-F5-HTTP_2.pdf
- 8.4.39 230-F5-BIG-IP-DNS-DATASHEET.pdf
- 8.4.40 231-F5-Route-Health-Injection.pdf
- 8.4.41 232-F5-IP-Anycast.pdf
- 8.4.42 233-F5-DNS Express-feature.pdf
- 8.4.43 234-F5-BIG-IP-DNS-operations-guide.pdf
- 8.4.44 235-F5-manual-resume-behavior-on-BIG-IP-DNS pools.pdf
- 8.4.45 236-F5-IPv6 Gateway-Module-and-Advanced-Routing-Module.pdf
- 8.4.46 237-F5-IPv4-and-IPv6-translation.pdf
- 8.4.47 238-F5-multiple-pool-resources-in-a-DNS-response.pdf
- 8.4.48 239-F5-Monitors-Concepts.pdf
- 8.4.49 240-F5-AFM-operations-guide.pdf
- 8.4.50 241-F5-Mitigating-DoS-Attacks.pdf
- 8.4.51 242-F5-Signature-Syntax.pdf
- 8.4.52 243-F5Creating-a-Simple-Security-Policy.pdf
- 8.4.53 244-F5-ASM-Policy-tuning-and-enhancement.pdf

- 8.4.54 245-F5-big-ip-application-security-manager-ds.pdf
- 8.4.55 246-F5-Secure-against-the-OWASP-Top-10.pdf
- 8.4.56 247-F5-ASM-CSRF-protection-feature.pdf
- 8.4.57 248-F5-HTTP-protocol-compliance.pdf
- 8.4.58 249-F5-cookie-tampering-protection.pdf
- 8.4.59 250-F5-block-requests-from-custom-User-Agent-using-ASM-iRule.pdf
- 8.4.60 259-F5-ASM-Attack-signature-Systems-and- Attack Type.pdf
- 8.4.61 260-F5-Custom-ASM-block-page.pdf
- 8.4.62 261-F5-Mitigating-Brute-Force-Attacks.pdf
- 8.4.63 262-F5-HTTP-methods-in-the-security-policy.pdf
- 8.4.64 263-F5-Blocking-malicious-traffic-using-the-IP-Intelligence-feature-in-BIG-IP-AFM.pdf
- 8.4.65 264-F5-AFM-Firewall-rules.pdf
- 8.4.66 265-F5-Fully-Automatic-Policy-Building-learning-mode.pdf
- 8.4.67 266-F5-Refining-Security-Policies-with-Learning.pdf
- 8.4.68 267-F5-Assigning-Attack-Signatures-to-Security-Policies.pdf
- 8.4.69 268-F5-Configuring-the-BIG-IP-System-as-a-Reverse-Proxy-Server.pdf
- 8.4.70 269-F5-Overview-of-the-Standard-virtual-server.pdf
- 8.4.71 270-F5-Multiple-HTTPS-sites-using-the-TLS-Server-Name-Indication-feature.pdf
- 8.4.72 271-F5-Changing-Security-Policy-Settings.pdf
- 8.4.73 272-F5-Configuration-changes-to-local-traffic-objects-do-not-affect-existing-connections.pdf
- 8.4.74 273-F5-XFF-HTTP-header.pdf
- 8.4.75 274-F5-Configuring-the-HTTP-profile-to-insert-a-custom-HTTP-header.pdf
- 8.4.76 275-F5-Setting-Up-Application-Statistics-Collection.pdf
- 8.4.77 275-Setting-Up-Application-Statistics-Collection.pdf
- 8.4.78 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf
- 8.4.79 277-F5-Scheduling-Reports.pdf
- 8.4.80 278-F5-IP-Intelligence.pdf
- 8.4.81 279-F5-Configuring-Bot Defense.pdf
- 8.4.82 280-F5-Detecting-and-mitigating-cyberattack-campaigns.pdf
- 8.4.83 281-F5-Event-Messages-and-Attack-Types.pdf
- 8.4.84 282-F5-Data-Guard.pdf
- 8.4.85 283-F5-Implementing-Web-Services-Security.pdf

- 8.4.86 284-F5-Creating-Login-Pages-for-Secure-Application-Access.pdf
- 8.4.87 285-F5-Configuring-advanced-encryption-on-a-URL-or-view.pdf
- 8.4.88 286-F5-big-ip-advanced-firewall-manager-datasheet.pdf
- 8.4.89 287-F5-Configuring-Access-Control-Lists.pdf
- 8.4.90 288-F5-Advanced-Firewall-Manager.pdf
- 8.4.91 289-F5-Investigating-BIG-IP-AFM-attack-vector-logs.pdf
- 8.4.92 290-F5- iRules_Programming-with-Tcl- DevCentral.pdf
- 8.4.93 291-F5-AFM Reporting.pdf
- 8.4.94 292-F5-Detecting-and-Preventing-Web-Scraping.pdf
- 8.4.95 293-F5-BIG-IP-ASM-HTTP-response-code-filtering.pdf
- 8.4.96 294-F5-Viewing-DDoS-Reports-Statistics-and-Logs.pdf
- 8.4.97 295-F5-Configuring-SNMP-Traps.pdf
- 8.4.98 296-F5-Testing-Packets-with-Firewall-IP-Intelligence-and-DoS-Rules.pdf
- 8.4.99 297-F5-Advanced-WAF-overview.pdf
- 8.4.100 298-F5-Kerberos-Authentication-with-End-Users-Logons.pdf
- 8.4.101 299-F5-Single-Sign-On-Methods.pdf
- 8.4.102 300-F5-Configuring-BIG-IP-APM-Kerberos-SSO-constrained-delegation-for-portal-access.pdf
- 8.4.103 301-F5-access-policy-manager-apm-overview.pdf
- 8.4.104 302-F5-big-ip-access-policy-manager-ds.pdf
- 8.4.105 303-F5-APM-Authentication Concepts.pdf
- 8.4.106 304-F5-configuring-Per-App-VPN-with-APM-and-F5-Access.pdf
- 8.4.107 305-F5-Configuring-Network-Access-Resources.pdf
- 8.4.108 306-F5-big-ip-local-traffic-manager-ds.pdf
- 8.4.109 307-F5-Optimize-Network-Access VPN.pdf
- 8.4.110 308-F5-APM-operations-guide.pdf
- 8.4.111 309-F5-About-Windows-Protected-Workspace.pdf
- 8.4.112 310-F5-About-Network-Access.pdf
- 8.4.113 311-F5-SSL-Traffic-Management.pdf
- 8.4.114 312-F5-SSL-Methods.pdf
- 8.4.115 313-F5-Using-Certificate-Authentication-in-APM.pdf
- 8.4.116 314-F5-Overview-of-the-hybrid SSL-acceleration-feature.pdf
- 8.4.117 315-F5-Configuring-SSL-connection-mirroring-for-Client-SSL-virtual-servers.pdf

- 8.4.118 316-F5-SSL-ciphers-supported-on-BIG-IP-platforms.pdf
- 8.4.119 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf
- 8.4.120 318-F5-Overview-of-the-SSL-Client-Certificate-Constrained-Delegation-feature.pdf
- 8.4.121 319-F5-Overview-of-the-Server-SSL-profile.pdf
- 8.4.122 320-F5-SSL-Orchestrator-SSL-Advanced-Configuration-Bypass-on-Handshake-Alert.pdf
- 8.4.123 321-F5-OCSP-Authentication.pdf
- 8.4.124 322-F5-Overview-of-BIG-IP-SSLTLS-cipher-suites.pdf
- 8.4.125 323-F5-Troubleshooting-SSLTLS-handshake-failures.pdf
- 8.4.126 324-F5-SSL-Certificate-Management.pdf
- 8.4.127 325-F5-What-CRL-formats-does-BIG-IP-support.pdf
- 8.4.128 326-F5-ssl-orchestrator-datasheet.pdf
- 8.4.129 327-F5-mitigating-ddos-attacks-tech-brief.pdf
- 8.4.130 328-F5-Configuring-Service-Chains.pdf
- 8.4.131 329-F5-Creating-Services-Service-Chains-and-Classifer-Rules.pdf
- 8.4.132 330-F5-Modify-the-F5-SSL-Orchestrator-service-monitor.pdf
- 8.4.133 331-F5-Implementing-SSL-Forward-Proxy-on-a-Single-BIG-IP-System.pdf
- 8.4.134 332-F5-Packet-Flow-in-an-SSL-Orchestrator-Reverse-Proxy.pdf
- 8.4.135 333-F5-Viewing-System-Level-Statistics.pdf
- 8.4.136 334-F5-Overview-of-BIG-IP-MIB-files.pdf
- 8.4.137 335-F5-iControl-SOAP-Home.pdf
- 8.4.138 336-F5-BIG-IP-AS3-API-Reference.pdf
- 8.4.139 337-F5-Viewing-Application-Page-Load-Times.pdf
- 8.4.140 338-F5-Troubleshooting-Applications-by-Capturing-traffic.pdf
- 8.4.141 339-F5-Using-Local-Traffic-Policies-with-Analytics.pdf
- 8.4.142 340-F5-User-roles.pdf
- 8.4.143 341-Monitoring-BIG-IP-System-Traffic-with-SNMP.pdf
- 8.4.144 342-F5-big-ip-virtual-editions-datasheet.pdf
- 8.4.145 343-F5-Prerequisites-for-BIG-IP-Virtual-Edition-on-ESXi.pdf

8.5 As seguintes “URLs” são partes integrantes da presente proposta:

Fabricante	Url
F5	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-afm-getting-started.html
F5	https://techdocs.f5.com/en-us/bigip-17-1-0/big-ip-system-dos-protection-and-protocol-firewall-implementations.html
F5	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-afm-nat.html
F5	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-network-firewall-policies-and-implementations.html
F5	https://my.f5.com/manage/s/article/K38201755
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/desktop-clientcompatmatrix.html
F5	https://techdocs.f5.com/en-us/apm-f5-access/apm-f5-access-android-3-0-9.html

Fabricante	Url
F5	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-access-policy-manager-advanced-customization-examples.html
F5	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-access-policy-manager-api-protection.html
F5	https://techdocs.f5.com/en-us/bigip-17-1-0/big-ip-access-policy-manager-application-access.html
F5	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-access-policy-manager-authentication-essentials.html
F5	https://techdocs.f5.com/en-us/bigip-17-5-0/big-ip-access-policy-manager-authentication-methods.html
F5	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-access-guard-config.html
F5	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-access-policy-manager-credential-protection.html
F5	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-access-policy-manager-customization.html
F5	https://techdocs.f5.com/en-us/edge-client-7-2-4/big-ip-access-policy-manager-edge-client-and-application-configuration-7-2-4.html
F5	https://techdocs.f5.com/en-us/edge-client-7-2-1/big-ip-edge-client-quick-start-macos-7-2-1.html
F5	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-access-policy-manager-implementations.html
F5	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-access-policy-manager-per-request-policies.html
F5	https://techdocs.f5.com/en-us/bigip-17-1-0/big-ip-access-policy-manager-network-access.html
F5	https://techdocs.f5.com/en-us/bigip-17-1-0/big-ip-access-policy-manager-oauth-configuration.html
F5	https://techdocs.f5.com/en-us/bigip-17-1-0/big-ip-access-policy-manager-portal-access.html
F5	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-access-policy-manager-priv-user-access.html
F5	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-access-policy-manager-saml-configuration.html
F5	https://techdocs.f5.com/en-us/bigip-17-1-0/big-ip-access-policy-manager-secure-web-gateway.html
F5	https://techdocs.f5.com/en-us/bigip-17-1-0/big-ip-access-policy-manager-single-sign-on-concepts-configuration.html
F5	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-access-policy-manager-third-party-integration.html
F5	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-access-policy-manager-visual-policy-editor.html
F5	https://techdocs.f5.com/en-us/apm-f5-access/apm-f5access-chromeos-1-0-0.html
F5	https://techdocs.f5.com/en-us/apm-f5-access/apm-f5-access-ios-3-0-1.html
F5	https://techdocs.f5.com/en-us/apm-f5-access/apm-f5-access-macos-2-0-0.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-clientcompatmatrix-17-5-1.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/related/edgeapps-clientcompatmatrix.html
F5	https://techdocs.f5.com/en-us/apm-f5-access/apm-f5-access-windows-10-using-intune.html
F5	https://my.f5.com/manage/s/article/K20775035
F5	https://my.f5.com/manage/s/article/K63942460
F5	https://clouddocs.f5.com/products/agc/8.0/
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/releasenotes/product/relnote-guided-config-10-0.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_apm/manuals/related/guided-config-compatmatrix-10-0.html
F5	https://clouddocs.f5.com/api/irules/ASM.html
F5	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-asm-attack-and-bot-signatures-14-1-0.html
F5	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-asm-getting-started.html
F5	https://techdocs.f5.com/en-us/bigip-17-5-0/big-ip-asm-implementations.html
F5	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-datasafe-configuration.html
F5	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-declarative-security-policy.html
F5	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-asm-implementations/common-elements-for-security-policies.html
F5	https://techdocs.f5.com/en-us/bigip-15-1-0/fraud-protection-service-big-ip-configuration.html
F5	https://my.f5.com/manage/s/article/K000141025
F5	https://my.f5.com/manage/s/article/K70941653
F5	https://my.f5.com/manage/s/article/K7922
F5	https://my.f5.com/manage/s/article/K85426947
F5	https://my.f5.com/manage/s/article/K07021938
F5	https://my.f5.com/manage/s/article/K000138861
F5	https://clouddocs.f5.com/products/waf-declarative-policy/v17_1.html
F5	https://my.f5.com/manage/s/article/K000135973
F5	https://my.f5.com/manage/s/article/K45215395
F5	https://my.f5.com/manage/s/article/K000149560
F5	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-analytics-implementations.html
F5	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-dns-services-implementations.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-concepts-12-0-0.html
F5	https://techdocs.f5.com/en-us/bigip-17-5-0/big-ip-dns-implementations.html
F5	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-dns-load-balancing.html
F5	https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-dns-monitors-reference.html
F5	https://my.f5.com/manage/s/article/K14510
F5	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-link-controller-implementations.html
F5	https://techdocs.f5.com/kb/en-us/products/lc_9_x/manuals/product/lc-monitors-reference-11-6-0.html
F5	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-local-traffic-management-basics-14-1-0.html
F5	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-local-traffic-management-getting-started-with-policies.html
F5	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-local-traffic-management-profiles-reference.html
F5	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-ltm-applying-a-pre-built-cipher-string-for-ssl-negotiation.html
F5	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-ltm-configuring-custom-cipher-string-for-ssl-negotiation.html
F5	https://techdocs.f5.com/en-us/bigip-17-0-0/big-ip-local-traffic-manager-implementations.html
F5	https://techdocs.f5.com/en-us/bigip-17-0-0/big-ip-local-traffic-management-internet-of-things-administration.html
F5	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-local-traffic-manager-monitors-reference.html
F5	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-service-provider-diameter-administration.html
F5	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-service-provider-generic-message-administration.html
F5	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-service-provider-message-routing-administration.html
F5	https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-service-provider-sip-administration-14-0-0.html
F5	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-http2-full-proxy-configuration.html
F5	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-http2-full-proxy-config-session-persistence.html
F5	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-icmp-health-monitor-traffic-prioritization.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-syn-flood-attacks-13-0-0.html
F5	https://my.f5.com/manage/s/article/K04597703

Fabricante	Url
F5	https://my.f5.com/manage/s/article/K55185917
F5	https://my.f5.com/manage/s/article/K93017176
F5	https://my.f5.com/manage/s/article/K10371011
F5	https://my.f5.com/manage/s/article/K7595
F5	https://my.f5.com/manage/s/article/K01155812
F5	https://my.f5.com/manage/s/article/K27310443
F5	https://my.f5.com/manage/s/article/K13675
F5	https://my.f5.com/manage/s/article/K15819
F5	https://my.f5.com/manage/s/article/K12015
F5	https://my.f5.com/manage/s/article/K8082
F5	https://my.f5.com/manage/s/article/K50411377
F5	https://my.f5.com/manage/s/article/K7535
F5	https://my.f5.com/manage/s/article/K14783
F5	https://my.f5.com/manage/s/article/K10251520
F5	https://my.f5.com/manage/s/article/K8802
F5	https://my.f5.com/manage/s/article/K75106155
F5	https://my.f5.com/manage/s/article/K14806
F5	https://my.f5.com/manage/s/article/K70671013
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/related/arm-bfd-command-reference-7-10-6.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/related/arm-bfd-configuration-7-10-6.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/related/arm-bgp-command-reference-7-10-6.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/related/arm-imi-command-reference-7-10-6.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/related/arm-isis-command-reference-7-10-6.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/related/arm-multicast-config-7-10-6.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/related/arm-nsm-command-reference-7-10-6.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/related/arm-ospf-command-reference-7-10-6.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/related/arm-pim-command-reference-7-10-6.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/related/arm-rip-command-reference-7-10-6.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/related/arm-troubleshooting-7-10-6.html
F5	https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-dynamic-routing-with-tmsh-and-icontrol-rest-14-0-0.html
F5	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-tmos-routing-administration-14-1-0.html
F5	https://my.f5.com/manage/s/article/K17721433
F5	https://my.f5.com/manage/s/article/K6654
F5	https://techdocs.f5.com/en-us/hardware/f5-rseries-systems-getting-started.html
F5	https://techdocs.f5.com/en-us/f5os-a-1-8-0/f5-rseries-systems-installation-upgrade.html
F5	https://techdocs.f5.com/en-us/f5os-a-1-8-0/f5-rseries-systems-administration-configuration.html
F5	https://techdocs.f5.com/en-us/hardware/platform-guide-r2000r4000-series.html
F5	https://techdocs.f5.com/en-us/hardware/platform-guide-r5000r10000-series.html
F5	https://techdocs.f5.com/en-us/hw-platforms/f5-rseries-systems-platform-diagnostics.html
F5	https://techdocs.f5.com/en-us/hw-platforms/f5-plat-accessories.html
F5	https://techdocs.f5.com/en-us/hw-platforms/installation-guide-f5optics-package.html
F5	https://clouddocs.f5.com/api/rseries-api/F5OS-A-1.8.0-cli.html
F5	https://clouddocs.f5.com/api/rseries-api/F5OS-A-1.8.0-api.html
F5	https://clouddocs.f5.com/f5os-error-catalog/rseries/f5os-a-1.8.0-errors.html
F5	https://techdocs.f5.com/en-us/bigip-17-5-0/ssl-orchestrator-setup.html
F5	https://techdocs.f5.com/en-us/bigip-17-5-0/big-ip-release-notes.html
F5	https://techdocs.f5.com/en-us/bigip-17-5-1/big-ip-release-notes.html
F5	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-device-service-clustering-administration-14-1-0.html
F5	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-digital-certificates-administration.html
F5	https://techdocs.f5.com/en-us/bigip-17-0-0/big-ip-system-and-net-hsm-implementation.html
F5	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-system-and-nshield-hsm-implementation.html
F5	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-system-and-safenet-luna-sa-hsm-implementation.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-ecmp-mirrored-clustering-12-1-0.html
F5	https://techdocs.f5.com/en-us/bigip-15-0-1/big-ip-system-configuring-geo-redundancy.html
F5	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-ltm-virtual-servers-multiple-ip-port.html
F5	https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-system-configuring-for-layer-2-transparency.html
F5	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-tunnels-vxlan-multipoint-ipv6-addressing.html
F5	https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-system-essentials.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-folders-administration-11-6-0.html
F5	https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-system-implementing-a-passive-monitoring-configuration.html
F5	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-system-initial-configuration.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-maintain-high-availability-through-resource-monitoring-13-0-0.html
F5	https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-system-migrating-devices-and-configurations-between-different-platforms.html
F5	https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-system-secure-password-policy.html
F5	https://techdocs.f5.com/en-us/bigip-17-5-0/big-ip-system-ssl-administration.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-upgrading-software-13-0-0.html
F5	https://techdocs.f5.com/en-us/bigip-17-0-0/big-ip-systems-user-account-administration.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-13-0-0.html
F5	https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-tmos-routing-administration-14-1-0.html
F5	https://techdocs.f5.com/en-us/bigip-17-1-0/big-ip-tmos-tunneling-and-ipsec.html
F5	https://techdocs.f5.com/en-us/bigip-15-0-0/external-monitoring-of-big-ip-systems-implementations.html
F5	https://clouddocs.f5.com/cloud/public/v1/matrix.html
F5	https://techdocs.f5.com/en-us/bigip-13-1-0/big-ip-secure-vault-administration.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/f5-amazon-cloudhsm-version-interoperability-matrix.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/f5-atos-hsm-version-interoperability-matrix.html

Fabricante	Url
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/f5-equinix-smartkey-hsm-version-interoperability-matrix.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/f5-ibm-hpcs-hsm-version-interoperability-matrix.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/f5-entrust-nshield-hsm-version-interoperability-matrix.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/f5-safenet-hsm-version-interoperability-matrix.html
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/f5-safenet-dpod-hsm-version-interoperability-matrix.html
F5	https://my.f5.com/manage/s/article/K000139252
F5	https://my.f5.com/manage/s/article/K000150065
F5	https://my.f5.com/manage/s/article/K000150714
F5	https://my.f5.com/manage/s/article/K00463541
F5	https://my.f5.com/manage/s/article/K13123
F5	https://my.f5.com/manage/s/article/K13205
F5	https://my.f5.com/manage/s/article/K16197
F5	https://my.f5.com/manage/s/article/K31539643
F5	https://my.f5.com/manage/s/article/K84002132
F5	https://my.f5.com/manage/s/article/K8759
F5	https://my.f5.com/manage/s/article/K9412
F5	https://my.f5.com/manage/s/article/K9476
F5	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/releases/related/log-messages.html
F5	https://my.f5.com/manage/s/article/K05939436
F5	https://my.f5.com/manage/s/article/K000136126
F5	https://my.f5.com/manage/s/article/K000134647
F5	https://my.f5.com/manage/s/article/K01770517
F5	https://my.f5.com/manage/s/article/K13213
F5	https://my.f5.com/manage/s/article/K15194
F5	https://clouddocs.f5.com/api/irules/
F5	https://clouddocs.f5.com/products/extensions/f5-appsvcs-extension/latest/
F5	https://clouddocs.f5.com/products/extensions/f5-declarative-onboarding/latest/
F5	https://clouddocs.f5.com/products/extensions/f5-appsvcs-templates/latest/
F5	https://clouddocs.f5.com/containers/latest/
F5	https://clouddocs.f5.com/products/orchestration/ansible/devel/
F5	https://github.com/F5Networks/f5-aws-cloudformation-v2
F5	https://github.com/F5Networks/f5-azure-arm-templates-v2
F5	https://github.com/F5Networks/f5-google-gdm-templates-v2
F5	https://clouddocs.f5.com/products/orchestration/terraform/latest/
F5	https://my.f5.com/manage/s/article/K13284
F5	https://clouddocs.f5.com/cloud/public/v1/
F5	https://techdocs.f5.com/en-us/bigip-17-1-0/big-ip-saas-bot-defense.html
F5	https://techdocs.f5.com/en-us/bigip-17-1-0/big-ip-dcs-client-side-defense-implementation.h

8.6 Planilha de Comprovação ponto-a-ponto:

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
	Grupo 1 (solução ADC física): Anexo I;	
1.	DOS REQUISITOS GERAIS	a) Conforme itens abaixo
1.1.	Modelo de referência: F5 Big-IP R4800 com Premium Service e Best Bundle, subscrição de IP Intelligence e ThreatCampaigns.(serão aceitas soluções de mesma marca e modelo ou de similares compatíveis e de qualidade superior, para que seja assegurada compatibilidade com a solução em uso no STJ).	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
1.2.	A solução é composta por 2 (dois) equipamentos do tipo ADC (Application Delivery Controller) com funções de Web Application Firewall (WAF), incluindo o fornecimento de transceivers, serviços de instalação, configuração, transferência de conhecimento, garantia e suporte técnico;	a) Proposta Técnica Comercial, Item 6 - Escopo de Fornecimento.
1.3.	O licenciamento de software do ADC deverá ser de uso perpétuo, exceto para funcionalidades relacionadas a atualizações periódicas de suas bases de inteligência que deverão ter seu funcionamento garantido até a expiração das licenças (vigência contratual). Dessa maneira, as atualizações de versões do ADC, o acesso à base de inteligência, bem como seu suporte e garantia serão interrompidos. Não obstante, as funcionalidades que não dependerem de atualizações periódicas deverão continuar funcionando plenamente.	a) Ciente e de acordo. b) Proposta Técnica Comercial, Item 6 - Escopo de Fornecimento. c) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
1.4.	Os equipamentos devem ser novos, de primeiro uso e estar em linha de fabricação na data de entrega da solução.	a) Ciente e de acordo.
1.5.	Devem possuir homologação da Agência Nacional de Telecomunicações (ANATEL) com validade indeterminada, conforme determina a Resolução nº 715, de 23 de outubro de 2019.	a) 011-ANATEL-Certificado-de-homologacao.pdf, página 1.
1.6.	Os hardwares e softwares ofertados na composição dos itens não devem estar listados como "End of Sale" e "End of Life" por seus respectivos fabricantes até a data da abertura das propostas.	a) 012-F5-hardware-product-lifecycle-support-policy, página 10.
1.6.1.	Durante a período da garantia, a CONTRATADA deverá manter todas as condições previstas em edital até o término da vigência contratual, devendo, inclusive, atualizar a solução integralmente por equipamentos compatíveis (com as especificações exigidas e com o equipamento originalmente ofertado), sem ônus adicional ao CONTRATANTE, caso a descontinuidade da solução se dê durante o período de garantia.	a) Ciente e de acordo.
1.7.	As versões de software dos equipamentos fornecidos devem ser disponibilizadas de forma global por seus fabricantes, com acesso amplo por parte da base de clientes, não sendo aceitas versões de software desenvolvidas de forma customizada para atendimento ao presente certame.	a) 030-F5-Download-products-from-MyF5.pdf, página 1 a 3. b) Ciente e de acordo.
1.8.	A partir do lançamento de uma atualização de software, os processos de mudança de versão podem ser especificados, controlados e executados pelo próprio cliente, com ou sem o apoio da CONTRATADA, sem prejuízo ao suporte às funcionalidades existentes;	a) 030-F5-Download-products-from-MyF5.pdf, página 1 a 3. b) Ciente e de acordo.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
1.9.	Para atendimento do Inciso III, Art. 3º do Decreto 7.174/2010, quando da entrega dos equipamentos, o licitante deverá comprovar a origem dos bens importados e apresentar comprovante de quitação dos tributos de importação a eles referentes, sob pena de suspensão do(s) pagamento(s), rescisão contratual e multa.	a) Ciente e de acordo.
1.10.	Por questões de compatibilidade, gerência, suporte e garantia, os equipamentos descritos neste anexo deverão ser de um mesmo fabricante, salvo disposto em contrário.	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12. b) Proposta Técnica Comercial, Item 6 - Escopo de Fornecimento.
1.11.	A solução deverá incluir quaisquer equipamentos e/ou componentes necessários ao pleno funcionamento e acomodação física, ambiental e lógica no ambiente do contratante, em conformidade com os padrões estabelecidos pelo fabricante.	a) Ciente e de acordo.
1.12.	Os equipamentos (hardware) deverão ser montados em bastidores (racks) de 19 (dezenove) polegadas (padrão EIA-310-D) e vir acompanhados de todos os acessórios para permitir essa montagem.	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
1.13.	A solução deve possuir memória RAM mínima de 64 GB.	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
1.14.	Deve possuir disco SSD com capacidade de armazenamento interno e retenção de logs para análise de no mínimo 480 GB.	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
1.15.	Deve possuir fontes de alimentação redundantes AC bivolt com as seguintes características:	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12. b) Conforme itens abaixo.
1.15.1.	Internas ao equipamento;	a) 013-F5-plataform-overview, página 3.
1.15.2.	Com ajuste automático de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12. b) 014-F5-Platform Specifications, página 3.
1.15.3.	Possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos.	a) 013-F5-plataform-overview, página 3.
1.15.4.	Ser capaz de sustentar a carga de todo o equipamento com todas as portas ativas, com apenas umas das fontes instalada.	a) 014-F5-Platform Specifications, página 5.
1.15.5.	Ser capaz de realizar a troca da fonte redundante com o equipamento em pleno funcionamento, sem nenhum impacto na performance (hot-swappable).	a) 014-F5-Platform Specifications, página 1.
1.15.6.	Vir acompanhadas com cabos de energia elétrica em conformidade com o padrão NBR14.136.	a) Ciente e de acordo.
1.15.7.	Permitir operação normal em temperaturas de 0°C até 40°C e umidade relativa de 5% a 85% (sem condensação);	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
1.16.	Deve possuir ventiladores redundantes;	a) 014-F5-Platform-Specifications.pdf, página 1.
1.17.	Cada equipamento deve possuir, no mínimo, 04 (quatro) portas 10 Gigabit Ethernet compatíveis com padrão RJ 45.	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
1.18.	Cada equipamento deve possuir, no mínimo, 04 (quatro) portas 25 Gigabit Ethernet compatíveis com transceivers SFP+ ou SFP28.	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
1.19.	Cada equipamento deve ser fornecido com os seguintes transceivers e cabos:	a) Conforme itens abaixo
1.19.1.	04 (quatro) transceivers SFP+ SR (velocidade 10 Gbps) ou 04 (quatro) transceivers SFP28-SR (velocidade 25 Gbps), conforme o critério do CONTRATANTE, para fibras multimodo com conectores do tipo LC duplex, incluindo o fornecimento dos cordões ópticos (OM4, no mínimo), com comprimento mínimo de 2,5m;	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12. b) Ciente e de acordo.
1.20.	Deve possuir, no mínimo, 01 (uma) porta de gerenciamento Ethernet 10/100/1000BASE-T, com conectores RJ-45. Esta porta será conectada na rede de gerência, permitindo a configuração de endereço IP próprio para gerenciamento. Deve permitir o acesso para gerenciamento do equipamento pelas demais portas.	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
1.21.	Deve ser possível configurar 02 (duas) das portas 10 Gigabit Ethernet para sincronização de heartbeat;	a) 015-F5-rSeries-High-Availability.pdf, páginas 1 e 2.
1.22.	Deve possuir recursos de agregação de portas baseado no protocolo LACP em seus modos ativo e passivo;	a) 016-F5-Network-Settings.pdf, página 4.
1.23.	Deve funcionar sob a forma de cluster composto por dois appliances físicos.	a) 015-F5-rSeries-High-Availability.pdf, páginas 1 e 2.
1.24.	O cluster deve operar tanto no modo ativo/passivo quanto no modo ativo/ativo;	a) 017-F5-Creating-an-Active-Active-Configuration-using-the-Configuration-Utility.pdf, página 1.
2.	DA CAPACIDADE E DESEMPENHO	a) Conforme itens abaixo
2.1.	Deve suportar, no mínimo, 40 (quarenta) Gbps de throughput em camada 7 e 50 (cinquenta) Gbps em camada 4 do modelo OSI;	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
2.2.	Deve suportar, no mínimo, 30 (trinta)Gbps de compressão em hardware para tráfego HTTP;	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
2.3.	Deve suportar, no mínimo, 1.800.000 (um milhão e oitocentos mil) requisições por segundo na camada 7 do modelo OSI;	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
2.4.	Deve suportar, no mínimo, 750.000 (setecentos e cinquenta mil) conexões por segundo na camada 4 do modelo OSI;	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
2.5.	Deve suportar, no mínimo, 38.000.000 (trinta e oito milhões) de conexões simultâneas na camada 4 do modelo OSI;	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
2.6.	Deve processar, no mínimo, 20.000 (vinte mil) transações SSL/TLS por segundo usando hardware especializado;	a) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
3.	DAS FUNCIONALIDADES	a) Conforme itens abaixo
3.1.	Deve possuir suporte a SMNPv3;	a) 040-F5-System Settings.pdf, página 17.
3.2.	Deve permitir autenticação em bases remotas por LDAP;	a) 050-F5-User-Management.pdf, página 3.
3.3.	Deve possuir três níveis de usuários de administração da solução: super usuário, usuário com permissões reduzidas e usuário com direito exclusivo a leitura;	a) 050-F5-User-Management.pdf, página 2.
3.4.	Deve ter a opção de armazenamento de registros de sistema (log) na solução ou em servidores externos;	a) 040-F5-System-Settings.pdf, página 7.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
3.5.	Dever possuir interface gráfica com usuário GUI (Graphic User Interface) acessível via navegador web e em conformidade com os padrões W3C, com acesso e operação por HTTPS por qualquer ponto da rede TCP/IP interna do contratante, que permita operação da solução e transferência de arquivos entre a solução e a máquina onde houve o acesso à GUI de maneira criptografada;	a) 060-F5-System-Overview.pdf, página 2.
3.6.	Deve possuir interface de linhas de comandos CLI (Command Line Interface) acessível e operável via SSH por qualquer ponto da rede TCP/IP interna, que permita operação da solução e transferência de arquivos entre a solução e sistemas externos de maneira criptografada;	a) 060-F5-System-Overview.pdf, página 2.
3.7.	Deve ter a capacidade de reinicialização remota da solução por GUI e/ou CLI;	a) 070-F5-Additional-System-Tasks.pdf, página 6.
3.8.	Deve ter a capacidade de aplicar atualizações preventivas, corretivas e de melhoria através da GUI e/ou CLI;	a) 040-F5-System-Settings.pdf, página 6.
3.9.	Deve possuir suporte à linguagem de programação ou interface (API) para automatização de atividades e configurações de sistemas, sem custo adicional;	a) 080-F5-iControlREST-Home.pdf, página 1.
3.10.	Deve ser disponibilizada documentação das APIs dos appliances que compõem a solução;	a) 090-F5-icontrol-rest-api-user-guide-16-1-0.pdf, páginas 1 a 131.
3.11.	Deve ser transparente quanto ao uso do protocolo IPv4 e IPv6 para a criação, modificação, remoção ou qualquer interação com equipamentos e servidores, reais ou virtuais;	a) 100-F5-Load-Balancing-to-IPv6-Nodes.pdf, página 2.
3.12.	Deve permitir o redirecionamento de páginas de erros 403, 404 e 50x específicas para páginas definidas pelo administrador;	a) 110-F5-Services-Profiles.pdf, página 2 e 3.
3.13.	Deve permitir que a solicitação de autenticação do cliente seja configurada conforme métodos abaixo:	a) Conforme itens abaixo
3.13.1.	Por certificado digital, enviando as informações do certificado (ex.: CN, DN) à aplicação de destino por header ou cookie específico.	a) 120-F5-On-Demand-Certificate-Authentication.pdf, página 7.
3.13.2.	Por formulário, verificando as credenciais via LDAP;	a) 130-F5-LDAP Query.pdf, páginas 1 a 6.
3.14.	Deve ser capaz de limitar o número de sessões estabelecidas com cada servidor real e virtual.	a) 140-F5-Preventing-TCP-Connection-Requests-From-Being-Dropped.pdf, páginas 1 e 2.
3.15.	Deve implementar Listas de Controle de Acesso (ACL), utilizando, no mínimo, os parâmetros de endereço IP de origem e destino.	a) 150-F5-packet-filtering.pdf, página 1.
3.16.	Deve oferecer proteção contra ataques de negação de serviço - Denial of Service (DoS) e Distributed Denial of Service (DDoS).	a) 160-F5-About-AFM-DoS_DDoS-Protection.pdf, página 1.
3.17.	Deve implementar limpeza de cabeçalho HTTP.	a) 170-F5-Remove-Server-Header-Information-in-HTTP-Responses.pdf, páginas 1 e 2.
3.18.	Deve possuir registro de logs com pelo menos as seguintes características:	a) Conforme itens abaixo
3.18.1.	Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;	a) 180-F5-Log-files-and-alerts.pdf, páginas 4 e 5.
3.18.2.	Os registros de log de acesso e eventos devem ser armazenados em arquivo ou banco de dados que permita a exportação ou em outro formato aberto CSV ou TXT, podendo ainda serem armazenados localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em servidor externo de banco de dados;	a) 190-F5-About-Logging.pdf, páginas 2 e 3.
3.18.3.	Permitir configurar a retenção dos logs por tempo e ou volume.	a) 180-F5-Log-files-and-alerts.pdf, páginas 8 e 9.
3.19.	Deve conter a funcionalidade de cache integrado, que tem por objetivo armazenar as respostas no cache interno para aliviar a carga de consumo de banda dos servidores.	a) 200-F5-Web-Acceleration.pdf, página 1.
3.20.	Deve possuir suporte a Virtual Extensible LAN (VXLAN).	a) 010-F5-application-delivery-controller-system-series-data-sheet.pdf, página 7.
3.21.	Deve se integrar com sistemas de gerenciamento de containers (ex.: Kubernetes/OpenShift), de modo a permitir que mudanças dinâmicas na infraestrutura de microsserviços sejam refletidas automaticamente no balanceamento de entrada, aumentando ou diminuindo a quantidade de pods, e ainda, inserindo ou removendo serviços do Big-IP.	a) 210-F5-Container-Ingress-Services.pdf, página 1.
3.22.	Deve ser integrado nativamente ao Kubernetes/OpenShift para realizar o balanceamento entre pods.	a) 220-F5-Service-Type-LoadBalancer.pdf
3.23.	Deve criar os serviços de Balanceamento de Carga dinamicamente ao mesmo tempo em que uma nova aplicação é provisionada pelo Kubernetes/OpenShift.	a) 210-F5-Container-Ingress-Services.pdf, página 1.
4.	DO BALANCEAMENTO LOCAL E GLOBAL	a) Conforme itens abaixo
4.1.	Não deve utilizar agentes ou qualquer outro tipo de aplicação instalada nos servidores ou clientes para executar suas funções e gerenciamento.	a) 010-F5-application-delivery-controller-system-series-data-sheet.pdf, página 12.
4.2.	Deve ser capaz de balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação.	a) 221-F5-Virtual-Server.pdf, página 1.
4.3.	Deve possuir, no mínimo, capacidade de resposta aos clientes por roteamento direto (os servidores balanceados respondem diretamente aos clientes), tunelamento (a solução é capaz de utilizar servidores de redes diferentes da que está inserida) ou full Proxy (todas as transações entre clientes e servidores são intermediadas pela solução).	a) 222-F5-reverse-proxy-server.pdf, página 1. b) 223-F5-SSL-Methods-for-LTM.pdf, páginas 1 e 2.
4.4.	Deve possuir, no mínimo, capacidade de balancear pelo menos 32 (trinta e dois) servidores virtuais por agrupamento (pool) vinculados a um VIP.	a) 224-F5-Maximum-number-of-members-allowed-in-a-pool.pdf, página 1.
4.5.	Deve ser capaz de operar com os seguintes algoritmos de balanceamento:	a) Conforme itens abaixo
4.5.1.	Fila circular simples (Round Robin - RR);	a) 225-F5-LTM-load-balancing.pdf, página 2.
4.5.2.	Fila circular ponderada (Weighted RR - WRR);	a) 225-F5-LTM-load-balancing.pdf, página 3.
4.5.3.	Menos conexões (Least Connections);	a) 225-F5-LTM-load-balancing.pdf, página 3.
4.5.4.	Servidor com resposta mais rápida;	a) 225-F5-LTM-load-balancing.pdf, página 4.
4.5.5.	Dinâmico, baseado em parâmetros do servidor coletados via SNMP.	a) 225-F5-LTM-load-balancing.pdf, página 11.
4.5.6.	Deve ser capaz de monitorar servidores reais e virtuais pelos seguintes métodos:	a) Conforme itens abaixo
4.5.6.1.	Portas TCP e UDP;	a) 225-F5-LTM-load-balancing.pdf, página 7.
4.5.6.2.	ICMP;	a) 225-F5-LTM-load-balancing.pdf, página 13.
4.5.6.3.	Conexões específicas de aplicação HTTP, HTTPS, FTP, RADIUS, SMTP, LDAP (em especial, Microsoft AD), POP3, SIP, SNMP. Caso a solução apresentada não possua algum desses monitores pré-configurados ("built in"), admitese sua criação customizada durante a fase de instalação.	a) 225-F5-LTM-load-balancing.pdf, página 7. b) 239-F5-Monitors-Concepts.pdf, página 1.
4.5.7.	Mesmo com a criação de novas sessões, deve garantir a persistência de sessões existentes entre clientes e servidores:	a) Conforme itens abaixo
4.5.7.1.	por análise da URL acessada;	a) 226-F5-Persistence-methods.pdf, página 2.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
4.5.7.2.	por análise de qualquer parâmetro no cabeçalho (header) HTTP;	a) 226-F5-Persistence-methods.pdf, página 2.
4.5.7.3.	por cookie - inserção de um novo cookie na sessão;	a) 226-F5-Persistence-methods.pdf, página 1.
4.5.7.4.	por cookie - utilização do valor do cookie da aplicação, sem adição de cookie;	a) 226-F5-Persistence-methods.pdf, página 1.
4.5.7.5.	por sessão SSL;	a) 226-F5-Persistence-methods.pdf, página 2.
4.5.7.6.	por endereço IP destino;	a) 226-F5-Persistence-methods.pdf, página 1.
4.5.7.7.	por endereço IP origem;	a) 226-F5-Persistence-methods.pdf, página 2.
4.5.7.8.	por análise do SIP Call ID.	a) 226-F5-Persistence-methods.pdf, página 2.
4.5.8.	Deve oferecer funcionalidades de otimização, cache proxy e compressão HTTP, com capacidade de:	a) Conforme itens abaixo
4.5.8.1.	Comprimir conteúdos HTTP (com o intuito de reduzir a quantidade de informações enviadas ao cliente);	a) 227-F5-Compression, página 1.
4.5.8.2.	Possibilitar uso de compressão de dados com formato GZIP;	a) 227-F5-Compression, página 3.
4.5.8.3.	Suportar a utilização e ajuste manual de quantidade memória RAM como cache proxy de objetos HTTP, para responder às requisições dos clientes sem utilizar recursos dos servidores;	a) 227-F5-Compression, página 3.
4.5.8.4.	Permitir a reescrita de requisições HTTP baseado no conteúdo da URL, possibilitando o redirecionamento de requisições HTTP para HTTPS;	a) 227-F5-Compression, página 2.
4.5.8.5.	Permitir a definição de quais tipos de objeto serão armazenados ou não em cache;	a) 110-F5-Services-Profiles.pdf, página 12.
4.5.8.6.	Permitir a reescrita de respostas HTTP, possibilitando a inclusão de cabeçalho (header) customizado;	a) 110-F5-Services-Profiles.pdf, página 5.
4.5.8.7.	Suportar multiplexação TCP e Reuso de Sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados;	a) 228-F5-OneConnect-profile.pdf, página 1 a 5.
4.5.8.8.	Suportar os protocolos HTTP, HTTP/1.1 e HTTP/2.0.	a) 229-F5-HTTP_2.pdf, página 1.
4.5.8.9.	Utilizar cache em memória RAM para maior velocidade no tempo de resposta;	a) 200-F5-Web-Acceleration.pdf, página 1.
4.5.9.	Deve suportar, no mínimo, as seguintes métricas para política de Balanceamento Global (GSLB):	a) Conforme itens abaixo
4.5.9.1.	Última resposta;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
4.5.9.2.	Status de saúde;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
4.5.9.3.	Número de servidores ativos em cada site;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
4.5.9.4.	Geolocalização;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
4.5.9.5.	Round Robin;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
4.5.9.6.	Número de sessões;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
4.5.9.7.	Connection Load do site;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
4.5.9.8.	Disponibilidade Global.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
4.5.10.	Deve suportar a realização de GSLB de forma transparente nos demais sites, desde que seja do mesmo fabricante e suportar mecanismos de visando Disaster Recovery e redundância entre Data Centers por meio de Route Health Injection (RHI).	a) 231-F5-Route-Health-Injection.pdf, página 1. b) 232-F5-IP-Anycast.pdf, páginas 1 a 3.
4.5.11.	Deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 2. b) 233-F5-DNS Express-feature.pdf, página 1.
4.5.12.	Deve servir às respostas as requisições onde o DNS é o autoritativo a partir da memória RAM; para este item, poderá ser aceita declaração do fabricante que comprove a funcionalidade.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 2. b) 233-F5-DNS Express-feature.pdf, página 1.
4.5.13.	Deve possuir proteções contra ataques DNS, no mínimo:	a) Conforme itens abaixo
4.5.13.1.	Pacotes malformados;	a) 240-F5-AFM-operations-guide.pdf, páginas 1, 2, 14, 15 e 16.
4.5.13.2.	Inspeção de Protocolo;	a) 240-F5-AFM-operations-guide.pdf, páginas 1, 2, 14, 15 e 16.
4.5.13.3.	UDP Flood;	a) 240-F5-AFM-operations-guide.pdf, páginas 1, 2, 14, 15 e 16. b) 241-F5-Mitigating-DoS-Attacks.pdf, páginas 1, 3 e 4.
4.5.13.4.	Validação de Protocolo;	a) 240-F5-AFM-operations-guide.pdf, páginas 1, 2, 14, 15 e 16. b) 241-F5-Mitigating-DoS-Attacks.pdf, páginas 1, 3 e 4.
4.5.13.5.	Ataque ICMP.	a) 240-F5-AFM-operations-guide.pdf, páginas 1, 2, 14, 15 e 16. b) 241-F5-Mitigating-DoS-Attacks.pdf, páginas 1, 3 e 4.
4.5.14.	Deve ser capaz de realizar filtragem de pacotes.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 4.
4.5.15.	Deve ser capaz de realizar IP Anycast.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 5.
4.5.16.	Deve ser capaz de realizar balanceamento dos servidores DNS.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 5.
4.5.17.	Deve ser capaz de realizar DNSSec, independente da estruturados servidores DNS em uso.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 5.
4.5.18.	Deve possuir alta disponibilidade, independente de BGP ou outro protocolo de roteamento. A alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, páginas 8 e 9.
4.5.19.	Deve aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, páginas 8 e 11.
4.5.20.	Deve ser possível ajustar quantos endereços são enviados em uma única resposta.	a) 238-F5-multiple-pool-resources-in-a-DNS-response.pdf, páginas 1 e 2.
4.5.21.	Deve suportar a monitoração de estado de saúde de servidores e serviços, garantindo a disponibilidade do serviço oferecido.	a) 239-F5-Monitors-Concepts.pdf, páginas 1 a 5.
4.5.22.	Deve operar, no mínimo, as seguintes formas:	a) Conforme itens abaixo
4.5.22.1.	DNSSec.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 5.
4.5.22.2.	Balanceamento de DNS Servers;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 5.
4.5.22.3.	DNS Autoritativo ou DNS Secundário;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 5.
4.5.23.	Deve implementar persistência de conexão do usuário entre aplicações ou data centers.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, páginas 7 e 8.
4.5.24.	Deve permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada.	a) 234-F5-BIG-IP-DNS-operations-guide.pdf, página 3.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
4.5.25.	Deve permitir que a contingência seja automática, mas que o retorno seja manual.	a) 235-F5-manual-resume-behavior-on-BIG-IP-DNS-pools.pdf, página 1.
4.5.26.	Deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6).	a) 236-F5-IPv6-Gateway-Module-and-Advanced-Routing-Module.pdf, páginas 1 e 2. b) 237-F5-IPv4-and-IPv6-translation.pdf, página 1.
5.	DOS REQUISITOS DE SEGURANÇA	a) Conforme itens abaixo
5.1.	Deve possuir as funcionalidades:	a) Conforme itens abaixo
5.1.1.	Deve ser independente de softwares proprietários (agentes) para a execução de quaisquer funções especificadas, bem como operar em alta disponibilidade independentemente de qualquer protocolo de roteamento.	a) 010-F5-application-delivery-controller-system-series-data-sheet.pdf, páginas 1 a 8. b) 015-F5-rSeries-High-Availability, páginas 1 a 6.
5.1.2.	Deve, no mínimo, permitir a criação de novas regras com parâmetros e expressões regulares definidos pelo administrador.	a) 242-F5-Signature-Syntax.pdf, páginas 9 a 11.
5.1.3.	Deve, no mínimo, permitir a criação de políticas diferenciadas por aplicação.	a) 243-F5-Creating-a-Simple-Security-Policy.pdf, páginas 1 e 2.
5.1.4.	Deve, no mínimo, permitir configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies.	a) 244-F5-ASM-Policy-tuning-and-enhancement.pdf, páginas 1 a 15.
5.1.5.	Deve, no mínimo, permitir a detecção e bloqueio de ataques a aplicação Web dos tipos abaixo:	a) Conforme itens abaixo
5.1.5.1.	SQL, Cookie e Command Injection;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
5.1.5.2.	Code Injection;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
5.1.5.3.	Violações do protocolo HTTP;	a) 248-F5-HTTP-protocol-compliance.pdf, páginas 1 a 3.
5.1.5.4.	Ameaças Web AJAX/JSON;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 3. b) 244-F5-ASM-Policy-tuning-and-enhancement.pdf, páginas 12 e 13.
5.1.5.5.	Cross-Site Scripting (XSS);	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
5.1.5.6.	Cross-Site Request Forgery;	a) 247-F5-ASM-CSRF-protection-feature.pdf, páginas 1 e 2.
5.1.5.7.	Buffer Overflow;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
5.1.5.8.	XML bombs/DoS;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
5.1.5.9.	Força bruta no browser;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12.
5.1.5.10.	Manipulação de campos escondidos e manipulação de cookies;	a) 249-F5-cookie-tampering-protection.pdf, páginas 1 e 2. b) 245-F5-big-ip-application-security-manager-ds.pdf, página 12.
5.1.5.11.	Cookie poisoning;	a) 249-F5-cookie-tampering-protection.pdf, páginas 1 e 2. b) 245-F5-big-ip-application-security-manager-ds.pdf, página 12.
5.1.5.12.	Sequestro de sessão;	a) 245-F5-big-ip-application-security-manager-ds.pdf, páginas 4 e 12.
5.1.5.13.	Checagem de cabeçalho do "user-agent" para identificar clientes inválidos.	a) 250-F5-block-requests-from-custom-User-Agent-using-ASM-iRule.pdf, página 1.
5.1.6.	Deve, no mínimo, permitir a detecção e bloqueio da resposta de determinada aplicação Web nos casos abaixo:	a) Conforme itens abaixo
5.1.6.1.	Ausência de tratamento de erros pela aplicação;	a) 293-F5-BIG-IP-ASM-HTTP-response-code-filtering.pdf, página 1.
5.1.6.2.	Vazamento de informações de infraestrutura.	a) 259-F5-ASM-Attack-signature-Systems-and-Attack-Type.pdf, página 6.
5.1.7.	Deve, no mínimo, permitir a customização da resposta de bloqueio.	a) 260-F5-Custom-ASM-block-page.pdf, página 1.
5.1.8.	Deve, no mínimo, proteger contra de ataques de força bruta em páginas de login.	a) 261-F5-Mitigating-Brute-Force-Attacks.pdf, página 1.
5.1.9.	Deve permitir o funcionamento do WAF usando o protocolo HTTP nas suas versões 1.0, 1.1 e 2 tanto do lado cliente quanto do lado servidor.	a) 229-F5-HTTP_2, páginas 1 a 6.
5.1.10.	Deve, no mínimo, permitir o bloqueio de métodos HTTP a critério do usuário.	a) 262-F5-HTTP-methods-in-the-security-policy.pdf, páginas 1 a 3.
5.1.11.	Deve, no mínimo, permitir o bloqueio de ataques no modo blacklisting e whitelisting.	a) 263-F5-Blocking-malicious-traffic-using-the-IP-Intelligence-feature-in-BIG-IP-AFM.pdf, páginas 1 a 3.
5.1.12.	Deve, no mínimo, permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.	a) 264-F5-AFM-Firewall-rules.pdf, página 8.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
5.1.13.	Deve, no mínimo, possuir funcionalidade de aprendizagem automática do funcionamento de uma aplicação web, suas URLs, parâmetros, dentre outras, para a configuração do bloqueio.	a) 265-F5-Fully-Automatic-Policy-Building-learning-mode.pdf, páginas 1 a 6.
5.1.14.	Deve, no mínimo, possuir funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação ou através de aprovação de regras pelo administrador.	a) 265-F5-Fully-Automatic-Policy-Building-learning-mode.pdf, páginas 1 a 6.
5.1.15.	Deve, no mínimo, permitir a customização, pelo administrador, dos parâmetros aprendidos, de forma a criar regras baseadas no tamanho do parâmetro, tipo de conteúdo, e expressões regulares.	a) 266-F5-Refining-Security-Policies-with-Learning.pdf, páginas 1 a 10. a) 242-F5-Signature-Syntax.pdf, páginas 9 a 11.
5.1.16.	Deve ser possível desabilitar algumas assinaturas específicas ou regras em determinados parâmetros, como uma exceção à regra geral.	a) 267-F5-Assigning-Attack-Signatures-to-Security-Policies.pdf, página 12.
5.1.17.	Deve, no mínimo, funcionar como proxy reverso de aplicações, incluindo a tradução de URLs para diferentes Servidores Virtuais.	a) 268-F5-Configuring-the-BIG-IP-System-as-a-Reverse-Proxy-Server.pdf, páginas 1 a 8.
5.1.18.	Deve, no mínimo, funcionar como proxy reverso de aplicações, incluindo a tradução de URLs para diferentes Servidores Virtuais. Appl	a) 268-F5-Configuring-the-BIG-IP-System-as-a-Reverse-Proxy-Server.pdf, páginas 1 a 8. b) 269-F5-Overview-of-the-Standard-virtual-server.pdf, páginas 1 a 15.
5.1.19.	Deve, no mínimo, permitir o mapeamento em um mesmo IP virtual, de acordo com a URL requisitada, que exija certificado digital de cliente para algumas aplicações e não exija para outras.	a) 270-F5-Multiple-HTTPS-sites-using-the-TLS-Server-Name-Indication-feature.pdf, páginas 1 a 6.
5.1.20.	Deve, no mínimo, permitir a configuração do modo para somente de detecção ou bloqueio, globalmente ou por cada regra.	a) 271-F5-Changing-Security-Policy-Settings.pdf, páginas 1 a 8.
5.1.21.	Deve, no mínimo, permitir a aplicação de novas regras sem interromper as conexões já abertas.	a) 272-F5-Configuration-changes-to-local-traffic-objects-do-not-affect-existing-connections.pdf, páginas 1 a 5.
5.1.22.	Deve, no mínimo, permitir a inclusão do IP do cliente no campo X-Forwarded-For.	a) 273-F5-XF-HTTP-header.pdf, páginas 1 a 4.
5.1.23.	Deve, no mínimo, permitir a inclusão de parâmetros customizados nos cabeçalhos (headers) HTTP, além da alteração dos existentes, para envio à aplicação de destino.	a) 274-F5-Configuring-the-HTTP-profile-to-insert-a-custom-HTTP-header.pdf, páginas 1 a 4.
5.1.24.	Deve, no mínimo, ter suporte a SNI (Server Name Indication).	a) 270-F5-Multiple-HTTPS-sites-using-the-TLS-Server-Name-Indication-feature.pdf, páginas 1 a 6.
5.1.25.	Deve, no mínimo, permitir no mínimo 32 servidores virtuais por agrupamento (pool) vinculados a cada endereço IP virtual (VIP).	a) 224-F5-Maximum-number-of-members-allowed-in-a-pool.pdf, página 1.
5.1.26.	Deve, no mínimo, permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios.	a) 110-F5-Services-Profiles.pdf, página 2.
5.1.27.	Deve, no mínimo, implementar proteção ao JSON (JavaScriptObject Notation).	a) 245-F5-big-ip-application-security-manager-ds.pdf, páginas 2 e 3.
5.1.28.	Deve, no mínimo, permitir a geração de relatórios customizados do módulo de Web Application Firewall, disponibilizando no mínimo os relatórios abaixo:	a) Conforme itens abaixo
5.1.28.1.	URL e endereços IPs.	a) 275-Setting-Up-Application-Statistics-Collection.pdf, página 5.
5.1.28.2.	Top Ataques (geral ou por aplicação/servidor);	a) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
5.1.28.3.	Tipos de Ataques;	a) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
5.1.28.4.	Severidade;	a) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
5.1.28.5.	Violações;	a) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
5.1.28.6.	Países;	a) 275-Setting-Up-Application-Statistics-Collection.pdf, página 5. b) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
5.1.28.7.	Top IPs de origem dos ataques;	a) 275-F5-Setting-Up-Application-Statistics-Collection.pdf, página 5. b) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
5.1.28.8.	Estatística de Tráfego;	a) 275-F5-Setting-Up-Application-Statistics-Collection.pdf, página 5. b) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
5.1.29.	Deve, no mínimo, permitir o agendamento e envio por e-mail dos relatórios, essa funcionalidade pode ser executada no equipamento ou pelo software de gerência.	a) 277-F5-Scheduling-Reports.pdf, páginas 1 a 4.
5.1.30.	Deve, no mínimo, permitir exportar os relatórios nos formatos HTML ou PDF.	a) 277-F5-Scheduling-Reports.pdf, páginas 1 a 4.
5.1.31.	Deve realizar a reputação de endereços IP, através de serviço de assinatura com atualização frequente online durante o período da garantia, impedindo que aplicações internas sejam acessadas por endereços IP maliciosos, botnets e proxys anônimos;	a) 278-F5-IP-Intelligence.pdf, páginas 1 a 4.
5.1.32.	A solução deve ser capaz de criar filtros de endereços IPs baseados em reputação, com no mínimo as seguintes categorias: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing, Proxy;	a) 278-F5-IP-Intelligence.pdf, páginas 1 a 4.
5.1.33.	Deve aplicar os filtros de reputação considerando o endereço IP e o cabeçalho HTTP X-Forwarded-For;	a) 278-F5-IP-Intelligence.pdf, páginas 1 a 4.
5.1.34.	Deve realizar a reputação de endereços IP, permitindo a configuração de whitelist para permitir a liberação de acessos considerados legítimos e de baixo risco;	a) 263-F5-Blocking-malicious-traffic-using-the-IP-Intelligence-feature-in-BIG-IP-AFM.pdf, páginas 1 a 3.
5.1.35.	Deve realizar proteção contra ataques automatizados, incluindo botnets, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma não operada por humanos;	a) 279-F5-Configuring-Bot-Defense.pdf, páginas 1 a 8.
5.1.36.	Deve realizar a identificação e bloqueio contra ataques sofisticados sem impactar nas transações das aplicações para os protocolos HTTP e HTTPS;	a) 346-F5-Configuring-Security-Policy-Blocking.pdf, página 1.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
5.1.37.	Deve realizar a identificação de ataques, contendo nome, campo atacado, quantidade de ataques, horário e endereços IPs envolvidos, através de relatórios históricos;	a) 279-Configuring-Bot Defense.pdf, páginas 1 a 8. b) 280-F5-Detecting-and-mitigating-cyberattack-campaigns.pdf, páginas 1 a 4.
5.1.38.	Deve identificar campanhas de ameaças usando base de conhecimento dinâmica e atualizada do fabricante para ameaças dinâmicas visando ataques de dia-zero.	a) 280-F5-Detecting-and-mitigating-cyberattack-campaigns.pdf, páginas 1 a 4.
5.1.39.	Deve possibilitar a correlação entre um incidente de ataque singular como parte de uma campanha de ameaça mais complexa e sofisticada.	a) 280-F5-Detecting-and-mitigating-cyberattack-campaigns.pdf, páginas 1 a 4.
5.1.40.	Para cada campanha identificada, deve informar no mínimo o nível de risco da campanha, o tipo de ataque, o endereço IP interno e qual VIP onde foram identificadas atividade relacionada à ameaça.	a) 281-F5-Event-Messages-and-Attack-Types.pdf, páginas 1 a 20.
5.1.41.	Deve ser capaz de verificar listas de endereços de alto risco cibernético, frequentemente atualizadas, e prover inteligência de contexto analisando as requisições para identificar fontes de ameaças.	a) 278-F5-IP-Intelligence.pdf, páginas 1 a 4.
5.1.42.	Deve realizar a identificação de dados sensíveis em páginas WEB, tais como senhas de acesso, por meio de campos de formulário, e o mascaramento, de forma a ocultar essa informação nos logs gerados;	a) 282-F5-Data-Guard.pdf, páginas 1 e 2.
5.1.43.	Deve suportar criptografia de dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação.	a) 283-F5-Implementing-Web-Services-Security.pdf, páginas 1 a 8. b) 285-F5-Configuring-advanced-encryption-on-a-URL-or-view.pdf, páginas 1 e 2.
5.1.44.	Deve proteger o login e as credenciais dos usuários e com isso os dados da aplicação com criptografia.	a) 284-F5-Creating-Login-Pages-for-Secure-Application-Access.pdf, páginas 1 a 7. b) 283-F5-Implementing-Web-Services-Security.pdf, páginas 1 a 8. c) 282-F5-Data-Guard.pdf, páginas 1 e 2.
5.1.45.	Deve possuir uma proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque.	a) 279-Configuring-Bot Defense.pdf, páginas 1 a 8. b) 280-F5-Detecting-and-mitigating-cyberattack-campaigns.pdf, páginas 1 a 4.
5.1.46.	Deve ser possível proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário.	a) 284-F5-Creating-Login-Pages-for-Secure-Application-Access.pdf, páginas 1 a 7. b) 283-F5-Implementing-Web-Services-Security.pdf, páginas 1 a 8. c) 282-F5-Data-Guard.pdf, páginas 1 e 2.
5.1.47.	Deve ser possível proteger esses dados criptografados de malwares e keyloggers.	a) 285-F5-Configuring-advanced-encryption-on-a-URL-or-view.pdf, páginas 1 e 2.
5.1.48.	Deve ser possível identificar anomalias e mitigá-las, através da análise contínua de carga e monitoração de saúde de servidores.	a) 292-F5-Detecting-and-Preventing-Web-Scraping, páginas 1 a 12.
5.2.	Deve suportar as funcionalidades de segurança para proteção DDoS:	a) Conforme itens abaixo
5.2.1.	Suportar proteção contra todos os tipos de ataques Denial of Service (DoS e DDoS);	a) 286-F5-big-ip-advanced-firewall-manager-datasheet.pdf, páginas 1 a 15.
5.2.2.	Proteger de ataques DDoS que utilizem SSL;	a) 286-F5-big-ip-advanced-firewall-manager-datasheet.pdf, página 2.
5.2.3.	Aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS.	a) 240-F5-AFM-operations-guide.pdf, páginas 5, 11 e 12.
5.2.4.	Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.	a) 240-F5-AFM-operations-guide.pdf, páginas 18, 23, 24 e 25.
5.2.5.	Permitir proteção contra ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning.	a) 240-F5-AFM-operations-guide.pdf, páginas 13 e 26.
5.2.6.	Permitir proteger contra ataques de DNS DDoS utilizando mecanismo que bloqueie somente as requisições maliciosas e permita requisições legítimas aos domínios existentes.	a) 286-F5-big-ip-advanced-firewall-manager-datasheet.pdf, página 4.
5.2.7.	Suportar Network Address Translation (NAT);	a) 286-F5-big-ip-advanced-firewall-manager-datasheet.pdf, página 6.
5.2.8.	Limitar o número de conexões;	a) 240-F5-AFM-operations-guide.pdf, páginas 5 a 8.
5.2.9.	Suportar Listas de Controle de Acesso (ACL);	a) 287-F5-Configuring-Access-Control-Lists.pdf, páginas 1 a 5. b) 288-F5-Advanced-Firewall-Manager.pdf, página 1.
5.2.10.	Permitir o log de ataques do tipo DoS;	a) 286-F5-big-ip-advanced-firewall-manager-datasheet.pdf, página 4, 7 e 9. b) 289-F5-Investigating-BIG-IP-AFM-attack-vector-logs.pdf, página 1.
5.2.11.	Possuir ferramenta flexível baseado em linguagem de programação open-source para customizar e aumentar o nível de segurança contra ataques DDoS, incluindo a possibilidade de interação com base de reputação de endereços IP e estatísticas de tráfego.	a) 290-F5-iRules_Programming-with-Tcl-DevCentral.pdf, páginas 1 a 3.
5.2.12.	Suportar relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DoS e DDoS.	a) 291-F5-AFM Reporting.pdf, páginas 1 a 3.
5.2.12.1.	Os relatórios devem indicar, no mínimo, a aplicação sendo atacada, o número de transações por aplicação e a latência da aplicação.	a) 294-F5-Viewing-DDoS-Reports-Statistics-and-Logs.pdf, página
5.2.13.	Possuir suporte ao envio de SNMP traps para cada ataque DDoS detectado.	a) 295-F5-Configuring-SNMP-Traps.pdf, página 1 a 4.
5.2.14.	Possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes com atributos específicos através da solução anti-DoS.	a) 296-F5-Testing-Packets-with-Firewall-IP-Intelligence-and-DoS-Rules.pdf, páginas 1 a 6.
5.2.15.	Ser possível a configuração do sistema para detectar e mitigar assinaturas dinâmicas. Quando configurado o sistema deve detectar possíveis ameaças DoS baseado no histórico do tráfego e poderá automaticamente mitigar essas ameaças.	a) 297-F5-Advanced-WAF-overview, página 1.
5.3.	Deve fornecer acesso seguro as aplicações:	a) Conforme itens abaixo

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
5.3.1.	Deve ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeiram autenticação;	a) 299-F5-Single-Sign-On-Methods.pdf, página 1.
5.3.2.	Deve ser capaz de realizar Single Sign On utilizando KERBEROS;	a) 298-F5-Kerberos-Authentication-with-End-Users-Logons.pdf, página 1.
5.3.3.	Deve ser capaz de fazer cache das credenciais do usuário e utilizar a credencial correta para cada sistema;	a) 300-F5-Configuring-BIG-IP-APM-Kerberos-SSO-constrained-delegation-for-portal-access.pdf, página 1.
5.3.4.	Deve ser capaz de implementar SSO mesmo quando conectado via modo "Network", quando o usuário chama o portal digitando o site diretamente no browser (sem clicar pelo portal);	a) 301-F5-access-policy-manager-apm-overview.pdf, página 3.
5.3.5.	Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware;	a) 302-F5-big-ip-access-policy-manager-ds.pdf, página 3.
5.3.6.	Deve ser capaz de autenticar usuários em bases de dados LDAP, RADIUS, TACACS+, ou Active Directory;	a) 303-F5-APM-Authentication Concepts.pdf, página 1.
5.3.7.	Deve possuir o modo onde o usuário estabelece túnel somente para o tráfego da aplicação, não sendo permitido outro tipo de tráfego dentro do mesmo túnel;	a) 304-F5-configuring-Per-App-VPN-with-APM-and-F5-Access.pdf, página 1.
5.3.8.	Deve possuir modo onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;	a) 302-F5-big-ip-access-policy-manager-ds.pdf, página 2.
5.3.9.	Deve possuir o modo onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna;	a) 305-F5-Configuring-Network-Access-Resources.pdf, páginas 1 a 3.
5.3.10.	Deve possuir Suporte a compressão HTTP;	a) 306-F5-big-ip-local-traffic-manager-ds.pdf, página 9.
5.3.11.	Deve possuir suporte a split tunneling;	a) 305-F5-Configuring-Network-Access-Resources.pdf, páginas 5.
5.3.12.	Deve permitir estabelecimento de conexão segura de acesso remoto sem a necessidade de instalação de um software cliente na máquina do usuário;	a) 302-F5-big-ip-access-policy-manager-ds.pdf, página 5.
5.3.13.	Deve permitir a utilização do protocolo padrão HTTPS com SSL como transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento DTLS (Datagram TLS);	a) 307-F5-Optimize-Network-Access VPN, página 7 e 8.
5.3.14.	Deve possibilitar compressão de dados antes de sua criptografia;	a) 308-F5-APM-operations-guide.pdf, página 14.
5.3.15.	Deve possibilitar utilização de área de trabalho protegida, onde os arquivos de trabalho devem ser criptografados e, ao fim de cada sessão, removidos automaticamente para garantir o máximo nível de segurança;	a) 302-F5-big-ip-access-policy-manager-ds.pdf, página 5. b) 309-F5-About-Windows-Protected-Workspace.pdf, página 1.
5.3.16.	Deve possibilitar a customização da interface gráfica da página de Login e mensagens de apresentação ao usuário;	a) 302-F5-big-ip-access-policy-manager-ds.pdf, página 10.
5.3.17.	Deve oferecer acesso remoto seguro à rede inteira para qualquer aplicação baseada em IP (TCP ou UDP);	a) 310-F5-About-Network-Access, página 1 a 3.
6.	DO TRATAMENTO DE TRÁFEGO SSL	a) Conforme itens abaixo
6.1.	Deve permitir a encriptação/decriptação de sessões SSL no lugar dos servidores (processo conhecido como SSL Offload);	a) 311-F5-SSL-Traffic-Management.pdf, página 1.
6.2.	Deve permitir que a terminação SSL/Troca de chaves/criptografia seja feita com aceleração em hardware;	a) 311-F5-SSL-Traffic-Management.pdf, página 27 e 34.
6.3.	Deve possibilitar encriptação até o servidor real;	a) 311-F5-SSL-Traffic-Management.pdf, páginas 1 e 9 a 15.
6.4.	Deve permitir que requisições HTTPS possam ser enviadas diretamente aos servidores por meio de protocolo HTTP aberto;	a) 311-F5-SSL-Traffic-Management.pdf, página 1 e 2.
6.5.	Deve possuir políticas de controle de acesso e autenticação baseadas nos atributos de certificado;	a) 313-F5-Using-Certificate-Authentication-in-APM.pdf, páginas 1 a 9.
6.6.	Deve permitir que o WAF "recriptografe" (em SSL/TLS, utilizando um certificado interno privado diferente do certificado válido) as requisições do cliente para o servidor real, antes destas serem para ele enviadas. Deve ser possível configurar um algoritmo e tamanho de chave distinto do utilizado no estabelecimento do túnel criptografado entre o cliente e o WAF;	a) 312-F5-SSL-Methods.pdf, página 3, 4 e 5.
6.7.	Implementar aceleração de TLS com instalação do certificado digital na solução, troca de chaves e criptografia dos dados assistida por hardware especializado.	a) 314-F5-Overview-of-the-hybrid-SSL-acceleration-feature.pdf, página 1.
6.7.1.	Permitir recriptografar a conexão entre a solução e o servidor;	a) 311-F5-SSL-Traffic-Management.pdf, página 1. b) 312-F5-SSL-Methods.pdf, página 3, 4 e 5.
6.7.2.	Permitir espelhamento de tráfego de conexões TLS;	a) 315-F5-Configuring-SSL-connection-mirroring-for-Client-SSL-virtual-servers.pdf, páginas 1 e 2.
6.7.3.	Suportar diversas cifras e protocolos SSL/TLS, incluindo TLS 1, 1.1, 1.2, 1.3, Forward Secrecy/Perfect Forward Secrecy, RSA, ECDSA, DHE, ECDHE, AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA, SHA2 (SHA256/384) e ChaCha20-Poly1305;	a) 316-F5-SSL-ciphers-supported-on-BIG-IP-platforms.pdf, páginas 1 a 19.
6.8.	Em relação ao tráfego TLS, deve suportar:	a) Conforme itens abaixo
6.8.1.	Autenticação do servidor pelo cliente, apresentando um certificado previamente configurado;	a) 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf, páginas 1 a 7.
6.8.2.	Autenticação do cliente pela solução, através da solicitação e verificação do certificado fornecido pelo cliente;	a) 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf, páginas 1 a 7.
6.8.3.	Autenticação mútua (mTLS), quando ambas as autenticações acima mencionadas ocorrendo de forma simultânea;	a) 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf, páginas 1 a 7.
6.8.4.	Encaminhar ao servidor real via cabeçalho HTTP todo o certificado utilizado pelo cliente para se autenticar;	a) 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf, páginas 1 a 7.
6.8.5.	Encaminhar ao servidor real via cabeçalho HTTP atributos específicos do certificado utilizado pelo cliente;	a) 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf, páginas 1 a 7.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
6.8.6.	Se autenticar com o servidor utilizando um certificado de cliente, próprio da solução, com os mesmos atributos do certificado do cliente;	a) 318-F5-Overview-of-the-SSL-Client-Certificate-Constrained-Delegation-feature.pdf, páginas 1 e 2.
6.9.	As listas de acesso devem ser baseadas nos atributos de um certificado.	a) 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf, páginas 1 a 7.
6.10.	Deve permitir ações caso o certificado original do servidor não seja confiável ou esteja expirado;	a) 319-F5-Overview-of-the-Server-SSL-profile.pdf, página 7.
6.11.	Deve permitir "by-pass" do tráfego caso o TLS handshake falhe;	a) 320-F5-SSL-Orchestrator-SSL-Advanced-Configuration-Bypass-on-Handshake-Alert.pdf, páginas 1 e 2.
6.12.	Deve permitir a verificação da validade do certificado digital apresentado:	a) 321-F5-OCSP-Authentication, páginas 1 a 8.
6.12.1.	Pelo cliente através de Listas de Certificados Revogados (LCR) ou através de listas;	a) 321-F5-OCSP-Authentication, páginas 1 a 8.
6.12.2.	Via OCSP (Online Certificate Status Protocol);	a) 321-F5-OCSP-Authentication, páginas 1 a 8.
6.13.	Deve usar sempre o último arquivo LCR para a consulta de Lista de Certificados Revogados;	a) 321-F5-OCSP-Authentication, páginas 1 a 8.
6.14.	Deve implementar os protocolos TLS versões 1.1, 1.2 e 1.3;	a) 316-F5-SSL-ciphers-supported-on-BIG-IP-platforms.pdf, páginas 1 a 19.
6.15.	Deve manter e gerenciar todo o tráfego criptografado com protocolo, TLS versões 1.1, 1.2 e 1.3;	a) 316-F5-SSL-ciphers-supported-on-BIG-IP-platforms.pdf, páginas 1 a 19.
6.16.	Deve implementar o algoritmo de hash SHA1;	a) 322-F5-Overview-of-BIG-IP-SSLTLS-cipher-suites.pdf, página 2.
6.17.	Deve implementar renegociação de sessão;	a) 323-F5-Troubleshooting-SSLTLS-handshake-failures.pdf, página 3
6.18.	Deve possuir os seguintes algoritmos de encriptação: 3DES, RSA, AES128 e AES-256, ECCDHE (P-256 e P-384) e algoritmo de autenticação ECDSA;	a) 322-Overview-of-BIG-IP-SSLTLS-cipher-suites.pdf, páginas 2 e 3. b) 316-F5-SSL-ciphers-supported-on-BIG-IP-platforms.pdf, páginas 1 a 19.
6.19.	Deve permitir geração de chaves RSA, enrollment de certificado, importação e exportação de chaves, certificados de servidores, e checagem de LCR (Lista de Certificados Revogados);	a) 324-F5-SSL-Certificate-Management.pdf, páginas 1 a 7. b) 325-F5-What-CRL-formats-does-BIG-IP-support.pdf, página 1.
6.20.	Por direcionamento inteligente de tráfego SSL entende-se a capacidade de abrir o tráfego SSL de entrada ("INBOUND") encaminhá-lo, de forma seletiva, levando em conta o contexto de serviço, às diferentes soluções de segurança que estão no ambiente de Data Center. No âmbito deste projeto serão exigidas, no mínimo, as integrações com as soluções de NG Firewall.	a) 326-F5-ssl-orchestrator-datasheet.pdf, página 3.
6.21.	Deve suportar pelo menos as seguintes cifras e protocolos: TLS 1.1, 1.2 e 1.3, SHA, SHA2, AES-GCM, AES;	a) 316-F5-SSL-ciphers-supported-on-BIG-IP-platforms.pdf, páginas 1 a 19.
6.22.	Deve implementar geração de chaves RSA, enrollment de certificado, importação e exportação de chaves, certificados de servidores.	a) 324-F5-SSL-Certificate-Management.pdf, páginas 1 a 7. b) 325-F5-What-CRL-formats-does-BIG-IP-support.pdf, página 1.
6.23.	Deve terminar as conexões SSL com a finalidade de inspecioná-las.	a) 311-F5-SSL-Traffic-Management.pdf, página 1. b) 312-F5-SSL-Methods.pdf, página 3, 4 e 5.
6.24.	Deve proteger de ataques de negação de serviço que utilizem SSL.	a) 327-F5-mitigating-ddos-attacks-tech-brief.pdf, página 10.
6.25.	Deve ser possível descobrir ameaças ocultas no SSL/TLS e prevenir ataques em vários estágios, usando as soluções de segurança já existentes assim como novas soluções que venham a ser adquiridas futuramente, independente de marca/modelo.	a) 326-F5-ssl-orchestrator-datasheet.pdf, páginas 1 e 2.
6.26.	Deve ter capacidade de gerenciar o tráfego SSL do lado do cliente para o servidor, ou seja, deve ser capaz de decifrar todo o tráfego de entrada.	a) 311-F5-SSL-Traffic-Management.pdf, página 1. b) 312-F5-SSL-Methods.pdf, página 3, 4 e 5.
6.27.	Deve suportar ECDHE, RSA e DHE com suporte a Forward Secrecy.	a) 316-F5-SSL-ciphers-supported-on-BIG-IP-platforms.pdf, páginas 1 a 19. b) 311-F5-SSL-Traffic-Management.pdf, página 4 e 10.
6.28.	Deve suportar SSL Forward Secrecy como uma forma de melhorar a segurança nas transações SSL/TLS. Deve ser capaz de criar múltiplos Service Chains.	a) 311-F5-SSL-Traffic-Management.pdf, página 4 e 10.
6.29.	Deve suportar a renegociação de sessão;	a) 328-F5-Configuring-Service-Chains.pdf, páginas 1 e 2.
6.30.	Deve possibilitar a monitoração e gerenciamento independente de cada dispositivo da cadeia de inspeção. Deve possuir um mecanismo de classificação contextual do tráfego que será enviado para cada dispositivo.	a) 326-F5-ssl-orchestrator-datasheet.pdf, páginas 1 e 2.
6.31.	Deve fazer a monitoração dos serviços dentro da camada de inspeção	a) 329-F5-Creating-Services-Service-Chains-and-Classifier-Rules.pdf, página 4.
6.32.	Deve permitir a resiliência dos serviços dentro da zona de inspeção, inclusive fazendo o balanceamento de carga entre múltiplos equipamentos do mesmo serviço.	a) 329-F5-Creating-Services-Service-Chains-and-Classifier-Rules.pdf, página 3.
6.33.	Deve permitir escalar os dispositivos de segurança com alta disponibilidade, usando testes de monitoração de saúde para identificar o estado de cada equipamento de segurança.	a) 330-F5-Modify-the-F5-SSL-Orchestrator-service-monitor.pdf, página 1.
6.34.	Deve ser possível prevenir ameaças de entrada (Data Center) e de saída(usuários), incluindo ataques de exploração, retorno de chamada e extração de dados.	a) 331-F5-Implementing-SSL-Forward-Proxy-on-a-Single-BIG-IP-System.pdf, página 1. b) 332-F5-Packet-Flow-in-an-SSL-Orchestrator-Reverse-Proxy.pdf, páginas 1 e 2.
7.	DO GERENCIAMENTO LOCAL	a) Conforme itens abaixo
7.1.	Deve possuir funcionalidade de emissão de relatório gerencial/estatístico dos acessos em ferramenta local ou remota, além do syslog ou log interno, que contenham, no mínimo:	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
7.1.1.	Quantidade de acessos por VIP;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
7.1.2.	Possuir MIB SNMP.	a) 334-F5-Overview-of-BIG-IP-MIB-files.pdf, página 1.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
7.1.3.	Quantidade de acessos por serviços e servidores;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
7.1.4.	Quantidade de usuários conectados;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
7.1.5.	Disponibilidade dos serviços/VIP;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
7.1.6.	Tempo de latência do cliente e servidor;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
7.1.7.	Throughput de requisição e resposta;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
7.1.8.	Transações por segundo;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
7.1.9.	Quantidade de requisições por período;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
7.1.10.	Quantidade de sessões;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
7.1.11.	Retenção de logs para análise posterior;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
7.2.	Deve ser disponibilizada documentação das API dos appliances que compõem a solução;	a) 335-F5-iControl-SOAP-Home, página 1. b) 336-F5-BIG-IP-AS3-API-Reference.pdf, página 1.
7.3.	Deve ser capaz de analisar a performance de aplicações web.	a) 337-F5-Viewing-Application-Page-Load-Times.pdf, página 1.
7.4.	Deve gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, troubleshooting, planejamento de capacidade e análise da experiência dos usuários finais no acesso às aplicações.	a) 338-F5-Troubleshooting-Applications-by-Capturing-traffic, páginas 1 e 2.
7.5.	Deve, a partir das informações coletadas, permitir a análise dos dados por aplicações, por URLs, por clientes e por servidores, permitindo, assim, a identificação mais precisa dos eventuais ofensores para atendimento da especificação.	a) 339-F5-Using-Local-Traffic-Policies-with-Analytics.pdf, página 1.
7.6.	Deve gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados. Caso a solução não possua este recurso nativamente poderá ser aceito solução de terceiros para atendimento da especificação.	a) 339-F5-Using-Local-Traffic-Policies-with-Analytics.pdf, página 1. b) 345-F5-BIG-IP-APM-Client-Compatibility-Matrix.pdf, páginas 1 a 9.
7.7.	Deve permitir o detalhamento do tempo de resposta total de carregamento de uma URL/página.	a) 337-F5-Viewing-Application-Page-Load-Times.pdf, página 1.
7.8.	Deve suportar mecanismos para criar usuários com no mínimo três conjuntos distintos de privilégios, sendo um deles somente leitura das configurações, para acesso às funções de gerenciamento dos equipamentos, via protocolos SSH, SNMP ou HTTPS.	a) 340-F5-User-roles.pdf, páginas 1 a 5.
7.9.	Deve possibilitar a coleta de dados de gerenciamento dos equipamentos utilizando os protocolos SNMPv2c e SNMPv3.	a) 341-Monitoring-BIG-IP-System-Traffic-with-SNMP, páginas 1 e 2.
7.10.	Deve suportar MIB SNMP.	a) 334-F5-Overview-of-BIG-IP-MIB-files.pdf, página 1.
7.11.	Deve permitir a configuração de endereços IPs para o envio de traps SNMP (alarmes).	a) 295-F5-Configuring-SNMP-Traps.pdf, página 1 a 4.
Grupo 2 (solução ADC virtual): Anexo II.		
Appliance	Virtual Tipo 1 (uma unidade virtual – licenciamento/subscrições para 5 anos) · 1 x F5-BIG-VE-BTA-1G-V18 (BIGIP VIRTUAL EDITION: BEST BUNDLE 1 GBPS (V12.1.X V18.X)) · 2 x F5-SBS-BIGVE-IP121YR (BIG-IP Subscription: IP Intelligence License 1YR (VE-1G/VE-3G/VE-5G)) · 1 x F5-SBS-BIGVE-IP123YR (BIG-IP Subscription: IP Intelligence License 3YR (VE-1G/VE-3G/VE-5G)) · 2 x F5-SBS-BIG-VE-TC21YR (BIG-IP Subscription: Adv WAF Threat Campaigns License for VE 1YR (VE-1G)) · 1 x F5-SBS-BIG-VE-TC23YR (BIG-IP Subscription: Adv WAF Threat Campaigns License for VE 3YR (VE-1G))	a) Proposta Técnica Comercial, Item 6 - Escopo de Fornecimento.
1.	Características de desempenho e escalabilidade da unidade básica da solução:	a) Conforme itens abaixo
1.1	Possuir capacidade mínima para tratar 1 Gbps de throughput;	a) 342-F5-big-ip-virtual-editions-datasheet.pdf, página 11.
1.2	Suportar, no mínimo 2 vCPU em cada appliance;	a) 343-F5-Prerequisites-for-BIG-IP-Virtual-Edition-on-ESXi.pdf, página 1.
1.3	Deve suportar a configuração de, no mínimo, 04 (quatro) GB de memória RAM;	a) 343-F5-Prerequisites-for-BIG-IP-Virtual-Edition-on-ESXi.pdf, página 1.
1.4	Deve ser compatível com sistemas de virtualização VMware EXi 7 ou superior;	a) 343-F5-Prerequisites-for-BIG-IP-Virtual-Edition-on-ESXi.pdf, página 1.
1.5	Suportar 802.1q para o transporte de múltiplas VLAN por uma única porta e por um conjunto agregado de portas;	a) 343-F5-Prerequisites-for-BIG-IP-Virtual-Edition-on-ESXi.pdf, página 2.
1.6	A solução deve permanecer plenamente operante após o fim da garantia contratada, sem interrupção de tráfego ou funcionalidades, sendo admitido apenas o encerramento dos serviços de atualização de assinaturas e bases de inteligência;	a) Cliente e de acordo. b) 342-F5-big-ip-virtual-editions-datasheet.pdf, página 13
1.7	Os equipamentos desta solução devem ser appliances virtuais do mesmo fabricante, modelo, versão e licenciamento, sendo essa exigência requisito técnico fundamental para configuração de dispositivos que operarão em modo cluster;	a) Cliente e de acordo. b) Proposta Técnica Comercial, Item 6 - Escopo de Fornecimento.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
Appliance	Virtual Tipo 2 (uma unidade virtual - licenciamento/subscrições para 5 anos) · 1 x F5-BIG-VE-BTA-10G-V18 (BIGIP VIRTUAL EDITION: BEST BUNDLE 10 GBPS (V12.1.X V18.X)) · 2 x F5-SBS-BIGVE-IP131YR (BIG-IP Subscription: IP Intelligence License 1YR (VE-10G)) · 1 x F5-SBS-BIGVE-IP133YR (BIG-IP Subscription: IP Intelligence License 3YR (VE-10G)) · 2 x F5-SBS-BIG-VE-TC31YR (BIG-IP Subscription: Adv WAF Threat Campaigns License for VE 1YR (3G/High Performance VE)) · 1 x F5-SBS-BIG-VE-TC33YR (BIG-IP Subscription: Adv WAF Threat Campaigns License for VE 3YR (3G/High Performance VE))	a) Proposta Técnica Comercial, Item 6 - Escopo de Fornecimento.
1.	Características de desempenho e escalabilidade da unidade básica da solução:	a) Conforme itens abaixo
1.1	Possuir capacidade mínima para tratar 9 Gbps de throughput;	a) 342-F5-big-ip-virtual-editions-datasheet.pdf, página 11.
1.2	Suportar, no mínimo 8 vCPU em cada appliance;	a) 343-F5-Prerequisites-for-BIG-IP-Virtual-Edition-on-ESXi.pdf, página 1.
1.3	Deve suportar a configuração de, no mínimo, 16 (dezesesseis) GB de memória RAM;	a) 343-F5-Prerequisites-for-BIG-IP-Virtual-Edition-on-ESXi.pdf, página 1.
1.4	Deve ser compatível com sistemas de virtualização VMware ESXi 7 ou superior;	a) 343-F5-Prerequisites-for-BIG-IP-Virtual-Edition-on-ESXi.pdf, página 1.
1.5	Suportar 802.1q para o transporte de múltiplas VLAN por uma única porta e por um conjunto agregado de portas;	a) 343-F5-Prerequisites-for-BIG-IP-Virtual-Edition-on-ESXi.pdf, página 2.
1.6	A solução deve permanecer plenamente operante após o fim da garantia contratada, sem interrupção de tráfego ou funcionalidades, sendo admitido apenas o encerramento dos serviços de atualização de assinaturas e bases de inteligência;	a) Ciente e de acordo. b) 342-F5-big-ip-virtual-editions-datasheet.pdf, página 13
1.7	Os equipamentos desta solução devem ser appliances virtuais do mesmo fabricante, modelo, versão e licenciamento, sendo essa exigência requisito técnico fundamental para configuração de dispositivos que operarão em modo cluster;	a) Ciente e de acordo. b) Proposta Técnica Comercial, Item 6 - Escopo de Fornecimento.
	CARACTERÍSTICAS COMUNS PARA O TIPO 1 E TIPO 2	a) Conforme itens abaixo
1	DOS REQUISITOS GERAIS	a) Conforme itens abaixo
1.1	A solução é composta por 1 (um) appliance virtual do tipo ADC (Application Delivery Controller) com funções de Web Application Firewall (WAF), serviços de instalação, configuração, transferência de conhecimento, garantia e suporte técnico;	a) Proposta Técnica Comercial, Item 6 - Escopo de Fornecimento. b) 010-F5-application-delivery-controller-system-rseries-data-sheet.pdf, página 12.
1.2	O licenciamento de software do ADC deverá ser de uso perpétuo, exceto para funcionalidades relacionadas a atualizações periódicas de suas bases de inteligência que deverão ter seu funcionamento garantido até a expiração das licenças (vigência contratual). Dessa maneira, as atualizações de versões do ADC/WAF, o acesso à base de inteligência, bem como seu suporte e garantia serão interrompidos. Não obstante, as funcionalidades que não dependerem de atualizações periódicas deverão continuar funcionando plenamente.	a) Ciente e de acordo. b) Proposta Técnica Comercial, Item 6 - Escopo de Fornecimento. c) 342-F5-big-ip-virtual-editions-datasheet.pdf, páginas 1 e 2.
1.3	A composição dos itens não deve estar listados como "End of Sale" e "End of Life" por seus respectivos fabricantes até a data da abertura das propostas.	a) Ciente e de acordo. b) 344-F5-BIG-IP VE Version Plus license offerings.pdf, páginas 1 e 2.
1.4	Durante a período da garantia, a CONTRATADA deverá manter todas as condições previstas em edital até o término da vigência contratual, devendo, inclusive, atualizar a solução integralmente por outra compatível (com as especificações originalmente), sem ônus adicional ao CONTRATANTE, caso a descontinuidade da solução se dê durante o período de garantia.	a) Ciente e de acordo.
	As versões de software dos equipamentos fornecidos devem ser disponibilizadas de forma global por seus fabricantes, com acesso amplo por parte da base de clientes, não sendo aceitas versões de software desenvolvidas de forma customizada para atendimento ao presente certame.	a) 030-F5-Download-products-from-MyF5.pdf, página 1 a 3. b) Ciente e de acordo.
1.5	A partir do lançamento de uma atualização de software, os processos de mudança de versão podem ser especificados, controlados e executados pelo próprio cliente, com ou sem o apoio da CONTRATADA, sem prejuízo ao suporte às funcionalidades existentes;	a) 030-F5-Download-products-from-MyF5.pdf, página 1 a 3. b) Ciente e de acordo.
1.6	Para atendimento do Inciso III, Art. 3º do Decreto 7.174/2010, quando da entrega do objeto, o licitante deverá comprovar a origem dos bens importados e apresentar comprovante de quitação dos tributos de importação a eles referentes, sob pena de suspensão do(s) pagamento(s), rescisão contratual e multa.	a) Ciente e de acordo.
1.7	Por questões de compatibilidade, gerência, suporte e garantia, os objetos descritos neste anexo deverão ser de um mesmo fabricante, salvo disposto em contrário.	a) Ciente e de acordo. b) Proposta Técnica Comercial, Item 6 - Escopo de Fornecimento.
1.8	A solução deverá incluir quaisquer componentes necessários ao pleno funcionamento e acomodação física, ambiental e lógica no ambiente do contratante, em conformidade com os padrões estabelecidos pelo fabricante.	a) Ciente e de acordo.
1.9	Deve permitir operação em cluster tanto no modo ativo/passivo quanto no modo ativo/ativo;	a) 017-F5-Creating-an-Active-Active-Configuration-using-the-Configuration-Utility.pdf, página 1.
2	DAS FUNCIONALIDADES	a) Conforme itens abaixo
2.1	Deve possuir suporte a SMNPv3;	a) 040-F5-System Settings.pdf, página 17.
2.2	Deve permitir autenticação em bases remotas por LDAP;	a) 050-F5-User-Management.pdf, página 3.
2.3	Deve possuir três níveis de usuários de administração da solução: super usuário, usuário com permissões reduzidas e usuário com direito exclusivo a leitura;	a) 050-F5-User-Management.pdf, página 2.
2.4	Deve ter a opção de armazenamento de registros de sistema (log) na solução ou em servidores externos;	a) 040-F5-System-Settings.pdf, página 7.
2.5	Dever possuir interface gráfica com usuário GUI (Graphic User Interface) acessível via navegador web e em conformidade com os padrões W3C, com acesso e operação por HTTPS por qualquer ponto da rede TCP/IP interna do contratante, que permita operação da solução e transferência de arquivos entre a solução e a máquina onde houve o acesso à GUI de maneira criptografada;	a) 060-F5-System-Overview.pdf, página 2.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
2.6	Deve possuir interface de linhas de comandos CLI (Command Line Interface) acessível e operável via SSH por qualquer ponto da rede TCP/IP interna, que permita operação da solução e transferência de arquivos entre a solução e sistemas externos de maneira criptografada;	a) 060-F5-System-Overview.pdf, página 2.
2.7	Deve ter a capacidade de reinicialização remota da solução por GUI e/ou CLI;	a) 070-F5-Additional-System-Tasks.pdf, página 6.
2.8	Deve ter a capacidade de aplicar atualizações preventivas, corretivas e de melhoria através da GUI e/ou CLI;	a) 040-F5-System-Settings.pdf, página 6.
2.9	Deve possuir suporte à linguagem de programação ou interface (API) para automatização de atividades e configurações de sistemas, sem custo adicional;	a) 080-F5-iControlREST-Home.pdf, página 1.
2.10	Deve ser disponibilizada documentação das APIs dos appliances virtuais que compõem a solução;	a) 090-F5-icontrol-rest-api-user-guide-16-1-0.pdf, páginas 1 a 131.
2.11	Deve ser transparente quanto ao uso do protocolo IPv4 e IPv6 para a criação, modificação, remoção ou qualquer interação com equipamentos e servidores, reais ou virtuais;	a) 100-F5-Load-Balancing-to-IPv6-Nodes.pdf, página 2.
2.12	Deve permitir o redirecionamento de páginas de erros 403, 404 e 50x específicas para páginas definidas pelo administrador;	a) 110-F5-Services-Profiles.pdf, página 3.
2.13	Deve permitir que a solicitação de autenticação do cliente seja configurada conforme métodos abaixo:	a) Conforme itens abaixo
2.14	Por certificado digital, enviando as informações do certificado (ex.: CN, DN) à aplicação de destino por header ou cookie específico.	a) 120-F5-On-Demand-Certificate-Authentication.pdf, página 7.
2.15	Por formulário, verificando as credenciais via LDAP;	a) 130-F5-LDAP Query.pdf, páginas 1 a 6.
2.16	Deve ser capaz de limitar o número de sessões estabelecidas com cada servidor real e virtual.	a) 140-F5-Preventing-TCP-Connection-Requests-From-Being-Dropped.pdf, páginas 1 e 2.
2.17	Deve implementar Listas de Controle de Acesso (ACL), utilizando, no mínimo, os parâmetros de endereço IP de origem e destino.	a) 150-F5-packet-filtering.pdf, página 1.
2.18	Deve oferecer proteção contra ataques de negação de serviço - Denial of Service (DoS) e Distributed Denial of Service (DDoS).	a) 160-F5-About-AFM-DoS_DDoS-Protection.pdf, página 1.
2.19	Deve implementar limpeza de cabeçalho HTTP.	a) 170-F5-Remove-Server-Header-Information-in-HTTP-Responses.pdf
2.20	Deve possuir registro de logs com pelo menos as seguintes características:	a) Conforme itens abaixo
2.21	Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;	a) 180-F5-Log-files-and-alerts.pdf, páginas 4 e 5.
2.22	Os registros de log de acesso e eventos devem ser armazenados em arquivo ou banco de dados que permita a exportação ou em outro formato aberto CSV ou TXT, podendo ainda serem armazenados localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em servidor externo de banco de dados;	a) 190-F5-About-Logging.pdf, páginas 2 e 3.
2.23	Permitir configurar a retenção dos logs por tempo e ou volume.	a) 180-F5-Log-files-and-alerts.pdf, páginas 8 e 9.
2.24	Deve conter a funcionalidade de cache integrado, que tem por objetivo armazenar as respostas no cache interno para aliviar a carga de consumo de banda dos servidores.	a) 200-F5-Web-Acceleration.pdf, página 1.
2.25	Deve possuir suporte a Virtual Extensible LAN (VXLAN).	a) 010-F5-application-delivery-controller-system-series-data-sheet.pdf, página 12.
2.26	Deve se integrar com sistemas de gerenciamento de containers (ex.: Kubernetes/OpenShift), de modo a permitir que mudanças dinâmicas na infraestrutura de microsserviços sejam refletidas automaticamente no balanceamento de entrada, aumentando ou diminuindo a quantidade de pods, e ainda, inserindo ou removendo serviços do Big-IP.	a) 210-F5-Container-Ingress-Services.pdf, página 1.
2.27	Deve ser integrado nativamente ao Kubernetes/OpenShift para realizar o balanceamento entre pods.	a) 220-F5-Service-Type-LoadBalancer.pdf
2.28	Deve criar os serviços de Balanceamento de Carga dinamicamente ao mesmo tempo em que uma nova aplicação é provisionada pelo Kubernetes/OpenShift.	a) 210-F5-Container-Ingress-Services.pdf, página 1.
3	DO BALANCEAMENTO LOCAL E GLOBAL	a) Conforme itens abaixo
3.1	Não deve utilizar agentes ou qualquer outro tipo de aplicação instalada nos servidores ou clientes para executar suas funções e gerenciamento.	a) 010-F5-application-delivery-controller-system-series-data-sheet.pdf, página 7.
3.2	Deve ser capaz de balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação.	a) 221-F5-Virtual-Server.pdf, página 1.
3.3	Deve possuir, no mínimo, capacidade de resposta aos clientes por roteamento direto (os servidores balanceados respondem diretamente aos clientes), tunelamento (a solução é capaz de utilizar servidores de redes diferentes da que está inserida) ou full Proxy (todas as transações entre clientes e servidores são intermediadas pela solução).	a) 222-F5-reverse-proxy-server.pdf, página 1. b) 223-F5-SSL-Methods-for-LTM.pdf, páginas 1 e 2.
3.4	Deve possuir, no mínimo, capacidade de balancear pelo menos 32 (trinta e dois) servidores virtuais por agrupamento (pool) vinculados a um VIP.	a) 224-F5-Maximum-number-of-members-allowed-in-a-pool.pdf, página 1.
3.5	Deve ser capaz de operar com os seguintes algoritmos de balanceamento:	a) Conforme itens abaixo
3.5.1	Fila circular simples (Round Robin - RR);	a) 225-F5-LTM-load-balancing.pdf, página 2.
3.5.2	Fila circular ponderada (Weighted RR - WRR);	a) 225-F5-LTM-load-balancing.pdf, página 3.
3.5.3	Menos conexões (Least Connections);	a) 225-F5-LTM-load-balancing.pdf, página 3.
3.5.4	Servidor com resposta mais rápida;	a) 225-F5-LTM-load-balancing.pdf, página 4.
3.5.5	Dinâmico, baseado em parâmetros do servidor coletados via SNMP.	a) 225-F5-LTM-load-balancing.pdf, página 11.
3.5.6	Deve ser capaz de monitorar servidores reais e virtuais pelos seguintes métodos:	a) Conforme itens abaixo
3.5.7	Portas TCP e UDP;	a) 225-F5-LTM-load-balancing.pdf, página 7.
3.5.8	ICMP;	a) 225-F5-LTM-load-balancing.pdf, página 13.
3.5.9	Conexões específicas de aplicação HTTP, HTTPS, FTP, RADIUS, SMTP, LDAP (em especial, Microsoft AD), POP3, SIP, SNMP. Caso a solução apresentada não possua algum desses monitores pré-configurados ("built in"), admite-se sua criação customizada durante a fase de instalação.	a) 225-F5-LTM-load-balancing.pdf, página 7.
3.6	Mesmo com a criação de novas sessões, deve garantir a persistência de sessões existentes entre clientes e servidores:	a) Conforme itens abaixo
3.6.1	por análise da URL acessada;	a) 226-F5-Persistence-methods.pdf, página 2.
3.6.2	por análise de qualquer parâmetro no cabeçalho (header) HTTP;	a) 226-F5-Persistence-methods.pdf, página 2.
3.6.3	por cookie - inserção de um novo cookie na sessão;	a) 226-F5-Persistence-methods.pdf, página 1.
3.6.4	por cookie - utilização do valor do cookie da aplicação, sem adição de cookie;	a) 226-F5-Persistence-methods.pdf, página 1.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
3.6.5	por sessão SSL;	a) 226-F5-Persistence-methods.pdf, página 2.
3.6.6	por endereço IP destino;	a) 226-F5-Persistence-methods.pdf, página 1.
3.6.7	por endereço IP origem;	a) 226-F5-Persistence-methods.pdf, página 2.
3.6.8	por análise do SIP Call ID.	a) 226-F5-Persistence-methods.pdf, página 2.
3.7	Deve oferecer funcionalidades de otimização, cache proxy e compressão HTTP, com capacidade de:	a) Conforme itens abaixo
3.7.1	Comprimir conteúdos HTTP (com o intuito de reduzir a quantidade de informações enviadas ao cliente);	a) 227-F5-Compression, página 1.
3.7.2	Possibilitar uso de compressão de dados com formato GZIP;	a) 227-F5-Compression, página 3.
3.7.3	Suportar a utilização e ajuste manual de quantidade memória RAM como cache proxy de objetos HTTP, para responder às requisições dos clientes sem utilizar recursos dos servidores;	a) 227-F5-Compression, página 3.
3.7.4	Permitir a reescrita de requisições HTTP baseado no conteúdo da URL, possibilitando o redirecionamento de requisições HTTP para HTTPS;	a) 227-F5-Compression, página 2.
3.7.5	Permitir a definição de quais tipos de objeto serão armazenados ou não em cache;	a) 110-F5-Services-Profiles.pdf, página 12.
3.7.6	Permitir a reescrita de respostas HTTP, possibilitando a inclusão de cabeçalho (header) customizado;	a) 110-F5-Services-Profiles.pdf, página 5.
3.7.7	Suportar multiplexação TCP e Reuso de Sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados;	a) 228-F5-OneConnect-profile.pdf, página 1.
3.7.8	Suportar os protocolos HTTP, HTTP/1.1 e HTTP/2.0.	a) 229-F5-HTTP_2.pdf, página 1.
3.7.9	Utilizar cache em memória RAM para maior velocidade no tempo de resposta;	a) 200-F5-Web-Acceleration.pdf, página 1.
3.8	Deve suportar, no mínimo, as seguintes métricas para política de Balanceamento Global (GSLB):	a) Conforme itens abaixo
3.8.1	Última resposta;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
3.8.2	Status de saúde;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
3.8.3	Número de servidores ativos em cada site;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
3.8.4	Geolocalização;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
3.8.5	Round Robin;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
3.8.6	Número de sessões;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
3.8.7	Connection Load do site;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
3.8.8	Disponibilidade Global.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 9.
3.9	Deve suportar a realização de GSLB de forma transparente nos demais sites, desde que seja do mesmo fabricante e suportar mecanismos de visando Disaster Recovery e redundância entre Data Centers por meio de Route Health Injection (RHI).	a) 231-F5-Route-Health-Injection.pdf, página 1. b) 232-F5-IP-Anycast.pdf, páginas 1 a 3.
3.10	Deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 2. b) 233-F5-DNS Express-feature.pdf, página 1.
3.11	Deve servir às respostas as requisições onde o DNS é o autoritativo a partir da memória RAM; para este item, poderá ser aceita declaração do fabricante que comprove a funcionalidade.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 2. b) 233-F5-DNS Express-feature.pdf, página 1.
3.12	Deve possuir proteções contra ataques DNS, no mínimo:	a) Conforme itens abaixo
3.12.1	Pacotes malformados;	a) 240-F5-AFM-operations-guide.pdf, páginas 1, 2, 14, 15 e 16.
3.12.2	Inspeção de Protocolo;	a) 240-F5-AFM-operations-guide.pdf, páginas 1, 2, 14, 15 e 16.
3.12.3	UDP Flood;	a) 240-F5-AFM-operations-guide.pdf, páginas 1, 2, 14, 15 e 16. b) 241-F5-Mitigating-DoS-Attacks.pdf, páginas 1, 3 e 4.
3.12.4	Validação de Protocolo;	a) 240-F5-AFM-operations-guide.pdf, páginas 1, 2, 14, 15 e 16. b) 241-F5-Mitigating-DoS-Attacks.pdf, páginas 1, 3 e 4.
3.12.5	Ataque ICMP.	a) 240-F5-AFM-operations-guide.pdf, páginas 1, 2, 14, 15 e 16. b) 241-F5-Mitigating-DoS-Attacks.pdf, páginas 1, 3 e 4.
3.13	Deve ser capaz de realizar filtragem de pacotes.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 4.
3.14	Deve ser capaz de realizar IP Anycast.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 5.
3.15	Deve ser capaz de realizar balanceamento dos servidores DNS.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 5.
3.16	Deve ser capaz de realizar DNSSEC, independente da estrutura dos servidores DNS em uso.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 5.
3.17	Deve possuir alta disponibilidade, independente de BGP ou outro protocolo de roteamento. A alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, páginas 8 e 9.
3.18	Deve aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, páginas 8 e 11.
3.19	Deve ser possível ajustar quantos endereços são enviados em uma única resposta.	a) 238-F5-multiple-pool-resources-in-a-DNS-response.pdf, páginas 1 e 2.
3.20	Deve suportar a monitoração de estado de saúde de servidores e serviços, garantindo a disponibilidade do serviço oferecido.	a) 239-F5-Monitors-Concepts.pdf, páginas 1 a 5.
3.21	Deve operar, no mínimo, as seguintes formas:	a) Conforme itens abaixo
3.22	DNSSEC.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 5.
3.23	Balanceamento de DNS Servers;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 5.
3.24	DNS Autoritativo ou DNS Secundário;	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, página 5.
3.25	Deve implementar persistência de conexão do usuário entre aplicações ou data centers.	a) 230-F5-BIG-IP-DNS-Datasheet.pdf, páginas 7 e 8.
3.26	Deve permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada.	a) 234-F5-BIG-IP-DNS-operations-guide.pdf, página 3.
3.27	Deve permitir que a contingência seja automática, mas que o retorno seja manual.	a) 235-F5-manual-resume-behavior-on-BIG-IP-DNS-pools.pdf, página 1.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
3.28	Deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6).	a) 236-F5-IPv6-Gateway-Module-and-Advanced-Routing-Module.pdf, páginas 1 e 2. b) 237-F5-IPv4-and-IPv6-translation.pdf, página 1.
4	DOS REQUISITOS DE SEGURANÇA	a) Conforme itens abaixo
4.1	Deve ser independente de softwares proprietários (agentes) para a execução de quaisquer funções especificadas, bem como operar em alta disponibilidade independentemente de qualquer protocolo de roteamento, quando em cluster.	a) 010-F5-application-delivery-controller-system-series-data-sheet.pdf, páginas 1 a 8. b) 342-F5-big-ip-virtual-editions-datasheet.pdf, páginas 1 a 9.
4.2	Deve, no mínimo, permitir a criação de novas regras com parâmetros e expressões regulares definidos pelo administrador.	a) 242-F5-Signature-Syntax.pdf, páginas 9 a 11.
4.3	Deve, no mínimo, permitir a criação de políticas diferenciadas por aplicação.	a) 243-F5-Creating-a-Simple-Security-Policy.pdf, páginas 1 e 2.
4.4	Deve, no mínimo, permitir configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies.	a) 244-F5-ASM-Policy-tuning-and-enhancement.pdf, páginas 1 a 15.
4.5	Deve, no mínimo, permitir a detecção e bloqueio de ataques a aplicação Web dos tipos abaixo:	a) Conforme itens abaixo
4.5.1	SQL, Cookie e Command Injection;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
4.5.2	Code Injection;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
4.5.3	Violações do protocolo HTTP;	a) 248-F5-HTTP-protocol-compliance.pdf, páginas 1 a 3.
4.5.4	Ameaças Web AJAX/JSON;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 3. b) 244-F5-ASM-Policy-tuning-and-enhancement.pdf, páginas 12 e 13.
4.5.5	Cross-Site Scripting (XSS);	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
4.5.6	Cross-Site Request Forgery;	a) 247-F5-ASM-CSRF-protection-feature.pdf, páginas 1 e 2.
4.5.7	Buffer Overflow;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
4.5.8	XML bombs/DoS;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
4.5.9	Força bruta no browser;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12.
4.5.10	Manipulação de campos escondidos e manipulação de cookies;	a) 249-F5-cookie-tampering-protection.pdf, páginas 1 e 2. b) 245-F5-big-ip-application-security-manager-ds.pdf, página 12.
4.5.11	Cookie poisoning;	a) 249-F5-cookie-tampering-protection.pdf, páginas 1 e 2. b) 245-F5-big-ip-application-security-manager-ds.pdf, página 12.
4.5.12	Sequestro de sessão;	a) 245-F5-big-ip-application-security-manager-ds.pdf, páginas 4 e 12.
4.5.13	Checagem de cabeçalho do "user-agent" para identificar clientes inválidos.	a) 250-F5-block-requests-from-custom-User-Agent-using-ASM-iRule.pdf, página 1.
4.6	Deve, no mínimo, permitir configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies.	a) 244-F5-ASM-Policy-tuning-and-enhancement.pdf, páginas 1 a 15.
4.7	Deve, no mínimo, permitir a detecção e bloqueio de ataques a aplicações Web dos tipos abaixo:	a) Conforme itens abaixo
4.7.1	SQL, Cookie e Command Injection;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
4.7.2	Code Injection;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
4.7.3	Violações do protocolo HTTP;	a) 248-F5-HTTP-protocol-compliance.pdf, páginas 1 a 3.
4.7.4	Ameaças Web AJAX/JSON;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 3. b) 244-F5-ASM-Policy-tuning-and-enhancement.pdf, páginas 12 e 13.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
4.7.5	Cross-Site Scripting (XSS);	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
4.7.6	Cross-Site Request Forgery;	a) 247-F5-ASM-CSRF-protection-feature.pdf, páginas 1 e 2.
4.7.7	Buffer Overflow;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
4.7.8	XML bombs/DoS;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12. b) 246-F5-Secure-against-the-OWASP-Top-10 .pdf, página 3.
4.7.9	Força bruta no browser;	a) 245-F5-big-ip-application-security-manager-ds.pdf, página 12.
4.7.10	Manipulação de campos escondidos e manipulação de cookies;	a) 249-F5-cookie-tampering-protection.pdf, páginas 1 e 2. b) 245-F5-big-ip-application-security-manager-ds.pdf, página 12.
4.7.11	Cookie poisoning;	a) 249-F5-cookie-tampering-protection.pdf, páginas 1 e 2. b) 245-F5-big-ip-application-security-manager-ds.pdf, página 12.
4.7.12	Sequestro de sessão;	a) 245-F5-big-ip-application-security-manager-ds.pdf, páginas 4 e 12.
4.7.13	Checagem de cabeçalho do "user-agent" para identificar clientes inválidos.	a) 250-F5-block-requests-from-custom-User-Agent-using-ASM-iRule.pdf, página 1.
4.8	Deve, no mínimo, permitir a detecção e bloqueio da resposta de determinada aplicação Web nos casos abaixo:	a) Conforme itens abaixo
4.8.1	Ausência de tratamento de erros pela aplicação;	a) 293-F5-BIG-IP-ASM-HTTP-response-code-filtering.pdf, página 1.
4.8.2	Vazamento de informações de infraestrutura.	a) 259-F5-ASM-Attack-signature-Systems-and-Attack-Type.pdf, página 6.
4.9	Deve, no mínimo, permitir a customização da resposta de bloqueio.	a) 260-F5-Custom-ASM-block-page.pdf, página 1.
4.10	Deve, no mínimo, proteger contra de ataques de força bruta em páginas de login.	a) 261-F5-Mitigating-Brute-Force-Attacks.pdf, página 1.
4.11	Deve permitir o funcionamento do WAF usando o protocolo HTTP nas suas versões 1.0, 1.1 e 2, tanto do lado cliente quanto do lado servidor.	a) 229-F5-HTTP_2, páginas 1 a 6.
4.12	Deve, no mínimo, permitir o bloqueio de métodos HTTP a critério do usuário.	a) 262-F5-HTTP-methods-in-the-security-policy.pdf, páginas 1 a 3.
4.13	Deve, no mínimo, permitir o bloqueio de ataques no modo blacklisting e whitelisting.	a) 263-F5-Blocking-malicious-traffic-using-the-IP-Intelligence-feature-in-BIG-IP-AFM.pdf, páginas 1 a 3.
4.14	Deve, no mínimo, permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.	a) 264-F5-AFM-Firewall-rules.pdf, página 8.
4.15	Deve, no mínimo, possuir funcionalidade de aprendizagem automática do funcionamento de uma aplicação web, suas URLs, parâmetros, dentre outras, para a configuração do bloqueio.	a) 265-F5-Fully-Automatic-Policy-Building-learning-mode.pdf, páginas 1 a 6.
4.16	Deve, no mínimo, possuir funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação ou através de aprovação de regras pelo administrador.	a) 265-F5-Fully-Automatic-Policy-Building-learning-mode.pdf, páginas 1 a 6.
4.17	Deve, no mínimo, permitir a customização, pelo administrador, dos parâmetros aprendidos, de forma a criar regras baseadas no tamanho do parâmetro, tipo de conteúdo, e expressões regulares.	a) 266-F5-Refining-Security-Policies-with-Learning.pdf, páginas 1 a 10. a) 242-F5-Signature-Syntax.pdf, páginas 9 a 11.
4.18	Deve ser possível desabilitar algumas assinaturas específicas ou regras em determinados parâmetros, como uma exceção à regra geral.	a) 267-F5-Assigning-Attack-Signatures-to-Security-Policies.pdf, página 12.
4.19	Deve, no mínimo, funcionar como proxy reverso de aplicações, incluindo a tradução de URLs para diferentes Servidores Virtuais.	a) 268-F5-Configuring-the-BIG-IP-System-as-a-Reverse-Proxy-Server.pdf, páginas 1 a 8.
4.20	Deve, no mínimo, permitir o mapeamento de diversas aplicações em um mesmo IP virtual, enviando informações para conjuntos de servidores diferentes de acordo com a URL requisitada.	a) 268-F5-Configuring-the-BIG-IP-System-as-a-Reverse-Proxy-Server.pdf, páginas 1 a 8. b) 269-F5-Overview-of-the-Standard-virtual-server.pdf, páginas 1 a 15.
4.21	Deve, no mínimo, permitir o mapeamento em um mesmo IP virtual, de acordo com a URL requisitada, que exija certificado digital de cliente para algumas aplicações e não exija para outras.	a) 270-F5-Multiple-HTTPS-sites-using-the-TLS-Server-Name-Indication-feature.pdf, páginas 1 a 6.
4.22	Deve, no mínimo, permitir a configuração do modo para somente de detecção ou bloqueio, globalmente ou por cada regra.	a) 271-F5-Changing-Security-Policy-Settings.pdf, páginas 1 a 8.
4.23	Deve, no mínimo, permitir a aplicação de novas regras sem interromper as conexões já abertas.	a) 272-F5-Configuration-changes-to-local-traffic-objects-do-not-affect-existing-connections.pdf, páginas 1 a 5.
4.24	Deve, no mínimo, permitir a inclusão do IP do cliente no campo X-Forwarded-For.	a) 273-F5-XFF-HTTP-header.pdf, páginas 1 a 4.
4.25	Deve, no mínimo, permitir a inclusão de parâmetros customizados nos cabeçalhos (headers) HTTP, além da alteração dos existentes, para envio à aplicação de destino.	a) 274-F5-Configuring-the-HTTP-profile-to-insert-a-custom-HTTP-header.pdf, páginas 1 a 4.
4.26	Deve, no mínimo, ter suporte a SNI (Server Name Indication).	a) 270-F5-Multiple-HTTPS-sites-using-the-TLS-Server-Name-Indication-feature.pdf, páginas 1 a 6.
4.27	Deve, no mínimo, permitir no mínimo 32 servidores virtuais por agrupamento (pool) vinculados a cada endereço IP virtual (VIP).	a) 224-F5-Maximum-number-of-members-allowed-in-a-pool.pdf, página 1.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
4.28	Deve, no mínimo, permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios.	a) 110-F5-Services-Profiles.pdf, página 2.
4.29	Deve, no mínimo, implementar proteção ao JSON (JavaScriptObject Notation).	a) 245-F5-big-ip-application-security-manager-ds.pdf, páginas 2 e 3.
4.30	Deve, no mínimo, permitir a geração de relatórios customizados do módulo de Web Application Firewall, disponibilizando no mínimo os relatórios abaixo:	a) Conforme itens abaixo
4.30.1	URL e endereços IPs.	a) 275-Setting-Up-Application-Statistics-Collection.pdf, página 5.
4.30.2	Top Ataques (geral ou por aplicação/servidor);	a) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
4.30.3	Tipos de Ataques;	a) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
4.30.4	Severidade;	a) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
4.30.5	Violações;	a) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
4.30.6	Países;	a) 275-Setting-Up-Application-Statistics-Collection.pdf, página 5. b) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
4.30.7	Top IPs de origem dos ataques;	a) 275-F5-Setting-Up-Application-Statistics-Collection.pdf, página 5. b) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
4.30.8	Estatística de Tráfego;	a) 275-F5-Setting-Up-Application-Statistics-Collection.pdf, página 5. b) 276-F5-Displaying-Reports-and-Monitoring-ASM.pdf, páginas 1 a 6.
4.31	Deve, no mínimo, permitir o agendamento e envio por e-mail dos relatórios, essa funcionalidade pode ser executada no equipamento ou pelo software de gerência.	a) 277-F5-Scheduling-Reports.pdf, páginas 1 a 4.
4.32	Deve, no mínimo, permitir exportar os relatórios nos formatos HTML ou PDF.	a) 277-F5-Scheduling-Reports.pdf, páginas 1 a 4.
4.33	Deve realizar a reputação de endereços IP, através de serviço de assinatura com atualização frequente online durante o período da garantia, impedindo que aplicações internas sejam acessadas por endereços IP maliciosos, botnets e proxys anônimos;	a) 278-F5-IP-Intelligence.pdf, páginas 1 a 4.
4.34	A solução deve ser capaz de criar filtros de endereços IPs baseados em reputação, com no mínimo as seguintes categorias: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing, Proxy;	a) 278-F5-IP-Intelligence.pdf, páginas 1 a 4.
4.35	Deve aplicar os filtros de reputação considerando o endereço IP e o cabeçalho HTTP X-Forwarded-For;	a) 278-F5-IP-Intelligence.pdf, páginas 1 a 4.
4.36	Deve realizar a reputação de endereços IP, permitindo a configuração de whitelist para permitir a liberação de acessos considerados legítimos e de baixo risco;	a) 263-F5-Blocking-malicious-traffic-using-the-IP-Intelligence-feature-in-BIG-IP-AFM.pdf, páginas 1 a 3.
4.37	Deve realizar proteção contra ataques automatizados, incluindo botnets, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma não operada por humanos;	a) 279-F5-Configuring-Bot Defense.pdf, páginas 1 a 8.
4.38	Deve realizar a identificação e bloqueio contra ataques sofisticados sem impactar nas transações das aplicações para os protocolos HTTP e HTTPS;	a) 279-F5-Configuring-Bot Defense.pdf, páginas 1 a 8. b) 280-F5-Detecting-and-mitigating-cyberattack-campaigns.pdf, páginas 1 a 4.
4.39	Deve realizar a identificação de ataques, contendo nome, campo atacado, quantidade de ataques, horário e endereços IPs envolvidos, através de relatórios históricos;	a) 279-Configuring-Bot Defense.pdf, páginas 1 a 8. b) 280-F5-Detecting-and-mitigating-cyberattack-campaigns.pdf, páginas 1 a 4.
4.40	Deve identificar campanhas de ameaças usando base de conhecimento dinâmica e atualizada do fabricante para ameaças dinâmicas visando ataques de dia-zero.	a) 280-F5-Detecting-and-mitigating-cyberattack-campaigns.pdf, páginas 1 a 4.
4.41	Deve possibilitar a correlação entre um incidente de ataque singular como parte de uma campanha de ameaça mais complexa e sofisticada.	a) 280-F5-Detecting-and-mitigating-cyberattack-campaigns.pdf, páginas 1 a 4.
4.42	Para cada campanha identificada, deve informar no mínimo o nível de risco da campanha, o tipo de ataque, o endereço IP interno e qual VIP onde foram identificados atividade relacionada à ameaça.	a) 281-F5-Event-Messages-and-Attack-Types.pdf, páginas 1 a 20.
4.43	Deve ser capaz de verificar listas de endereços de alto risco cibernético, frequentemente atualizadas, e prover inteligência de contexto analisando as requisições para identificar fontes de ameaças.	a) 278-F5-IP-Intelligence.pdf, páginas 1 a 4.
4.44	Deve realizar a identificação de dados sensíveis em páginas WEB, tais como senhas de acesso, por meio de campos de formulário, e o mascaramento, de forma a ocultar essa informação nos logs gerados;	a) 282-F5-Data-Guard.pdf, páginas 1 e 2.
4.45	Deve suportar criptografia de dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação.	a) 283-F5-Implementing-Web-Services-Security.pdf, páginas 1 a 8. b) 285-F5-Configuring-advanced-encryption-on-a-URL-or-view.pdf, páginas 1 e 2.
4.46	Deve proteger o login e as credenciais dos usuários e com isso os dados da aplicação com criptografia.	a) 284-F5-Creating-Login-Pages-for-Secure-Application-Access.pdf b) 283-F5-Implementing-Web-Services-Security.pdf, páginas 1 a 8. c) 282-F5-Data-Guard.pdf, páginas 1 e 2.
4.47	Deve possuir uma proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque.	a) 279-Configuring-Bot Defense.pdf, páginas 1 a 8. b) 280-F5-Detecting-and-mitigating-cyberattack-campaigns.pdf, páginas 1 a 4.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
4.48	Deve ser possível proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário.	a) 284-F5-Creating-Login-Pages-for-Secure-Application-Access.pdf b) 283-F5-Implementing-Web-Services-Security.pdf, páginas 1 a 8. c) 282-F5-Data-Guard.pdf, páginas 1 e 2.
4.49	Deve ser possível proteger esses dados criptografados de malwares e keyloggers.	a) 285-F5-Configuring-advanced-encryption-on-a-URL-or-view.pdf, páginas 1 e 2.
4.50	Deve ser possível identificar anomalias e mitigá-las, através da análise contínua de carga e monitoração de saúde de servidores.	a) 292-F5-Detecting-and-Preventing-Web-Scraping, páginas 1 a 12.
4.51	Deve suportar as funcionalidades de segurança para proteção DDoS:	a) Conforme itens abaixo
4.51.1	Suportar proteção contra todos os tipos de ataques Denial of Service (DoS e DDoS);	a) 286-F5-big-ip-advanced-firewall-manager-datasheet.pdf, páginas 1 a 15.
4.51.2	Proteger de ataques DDoS que utilizem SSL;	a) 286-F5-big-ip-advanced-firewall-manager-datasheet.pdf, página 2.
4.51.3	Aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS.	a) 240-F5-AFM-operations-guide.pdf, páginas 5, 11 e 12.
4.51.4	Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.	a) 240-F5-AFM-operations-guide.pdf, páginas 18, 23, 24 e 25.
4.51.5	Permitir proteção contra ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning.	a) 240-F5-AFM-operations-guide.pdf, páginas 13 e 26.
4.51.6	Permitir proteger contra ataques de DNS DDoS utilizando mecanismo que bloqueie somente as requisições maliciosas e permita requisições legítimas aos domínios existentes.	a) 286-F5-big-ip-advanced-firewall-manager-datasheet.pdf, página 4.
4.51.7	Suportar Network Address Translation (NAT);	a) 286-F5-big-ip-advanced-firewall-manager-datasheet.pdf, página 6.
4.51.8	Limitar o número de conexões;	a) 240-F5-AFM-operations-guide.pdf, páginas 5 a 8.
4.51.9	Suportar Listas de Controle de Acesso (ACL);	a) 287-F5-Configuring-Access-Control-Lists.pdf, páginas 1 a 5. b) 288-F5-Advanced-Firewall-Manager.pdf, página 1.
4.51.10	Permitir o log de ataques do tipo DoS;	a) 286-F5-big-ip-advanced-firewall-manager-datasheet.pdf, página 4, 7 e 9. b) 289-F5-Investigating-BIG-IP-AFM-attack-vector-logs.pdf, página 1.
4.51.11	Possuir ferramenta flexível baseado em linguagem de programação open-source para customizar e aumentar o nível de segurança contra ataques DDoS, incluindo a possibilidade de interação com base de reputação de endereços IP e estatísticas de tráfego.	a) 290-F5-iRules_Programming-with-Tcl-DevCentral.pdf, páginas 1 a 3.
4.51.12	Suportar relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DoS e DDoS.	a) 291-F5-AFM-Reporting.pdf, páginas 1 a 3.
4.51.13	Os relatórios devem indicar, no mínimo, a aplicação sendo atacada, o número de transações por aplicação e a latência da aplicação.	a) 294-F5-Viewing-DDoS-Reports-Statistics-and-Logs.pdf, página
4.51.14	Possuir suporte ao envio de SNMP traps para cada ataque DDoS detectado.	a) 295-F5-Configuring-SNMP-Traps.pdf, página 1 a 4.
4.51.15	Possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes com atributos específicos através da solução anti-DoS.	a) 296-F5-Testing-Packets-with-Firewall-IP-Intelligence-and-DoS-Rules.pdf, páginas 1 a 6.
4.51.16	Ser possível a configuração do sistema para detectar e mitigar assinaturas dinâmicas. Quando configurado o sistema deve detectar possíveis ameaças DoS baseado no histórico do tráfego e poderá automaticamente mitigar essas ameaças.	a) 297-F5-Advanced-WAF-overview, página 1.
4.52	Deve fornecer acesso seguro as aplicações:	a) Conforme itens abaixo
4.52.1	Deve ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeiram autenticação;	a) 299-F5-Single-Sign-On-Methods.pdf, página 1.
4.52.2	Deve ser capaz de realizar Single Sign On utilizando KERBEROS;	a) 298-F5-Kerberos-Authentication-with-End-Users-Logons.pdf, página 1.
4.52.3	Deve ser capaz de fazer cache das credenciais do usuário e utilizar a credencial correta para cada sistema;	a) 300-F5-Configuring-BIG-IP-APM-Kerberos-SSO-constrained-delegation-for-portal-access.pdf, página 1.
4.52.4	Deve ser capaz de implementar SSO mesmo quando conectado via modo "Network", quando o usuário chama o portal digitando o site diretamente no browser (sem clicar pelo portal);	a) 301-F5-access-policy-manager-apm-overview.pdf, página 3.
4.52.5	Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware;	a) 302-F5-big-ip-access-policy-manager-ds.pdf, página 3.
4.52.6	Deve ser capaz de autenticar usuários em bases de dados LDAP, RADIUS, TACACS+, ou Active Directory;	a) 303-F5-APM-Authentication Concepts.pdf, página 1.
4.52.7	Deve possuir o modo onde o usuário estabelece túnel somente para o tráfego da aplicação, não sendo permitido outro tipo de tráfego dentro do mesmo túnel;	a) 304-F5-configuring-Per-App-VPN-with-APM-and-F5-Access.pdf, página 1.
4.52.8	Deve possuir modo onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;	a) 302-F5-big-ip-access-policy-manager-ds.pdf, página 2.
4.52.9	Deve possuir o modo onde um usuário se conecta efetivamente a rede interna, obtendo um endereço IP roteável pela rede interna;	a) 305-F5-Configuring-Network-Access-Resources.pdf, páginas 1 a 3.
4.52.10	Deve possuir Suporte a compressão HTTP;	a) 306-F5-big-ip-local-traffic-manager-ds.pdf, página 9.
4.52.11	Deve possuir suporte a split tunneling;	a) 305-F5-Configuring-Network-Access-Resources.pdf, páginas 5.
4.52.12	Deve permitir estabelecimento de conexão segura de acesso remoto sem a necessidade de instalação de um software cliente na máquina do usuário;	a) 302-F5-big-ip-access-policy-manager-ds.pdf, página 5.
4.52.13	Deve permitir a utilização do protocolo padrão HTTPS com SSL como transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento DTLS (Datagram TLS);	a) 307-F5-Optimize-Network-Access VPN, página 7 e 8.
4.52.14	Deve possibilitar de compressão de dados antes de sua criptografia;	a) 308-F5-APM-operations-guide.pdf, página 14.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
4.52.15	Deve possibilitar utilização de área de trabalho protegida, onde os arquivos de trabalho devem ser criptografados e, ao fim de cada sessão, removidos automaticamente para garantir o máximo nível de segurança;	a) 302-F5-big-ip-access-policy-manager-ds.pdf, página 5.
4.52.16	Deve possibilitar a customização da interface gráfica da página de Login e mensagens de apresentação ao usuário;	a) 302-F5-big-ip-access-policy-manager-ds.pdf, página 10.
4.52.17	Deve oferecer acesso remoto seguro a rede inteira para qualquer aplicação baseada em IP (TCP ou UDP);	a) 309-F5-About-Windows-Protected-Workspace.pdf, página 1.
5	DO TRATAMENTO DE TRÁFEGO SSL	a) Conforme itens abaixo
5.1	Deve permitir a encriptação/decriptação de sessões SSL no lugar dos servidores (processo conhecido como SSL Offload);	a) F5-311-SSL-Traffic-Management.pdf, página 1.
5.2	Deve permitir que a terminação SSL/Troca de chaves/criptografia seja feita com aceleração em hardware;	a) F5-311-SSL-Traffic-Management.pdf, página 27 e 34.
5.3	Deve possibilitar encriptação até o servidor real;	a) F5-311-SSL-Traffic-Management.pdf, páginas 1 e 9 a 15.
5.4	Deve permitir que requisições HTTPS possam ser enviadas diretamente aos servidores por meio de protocolo HTTP aberto;	a) F5-311-SSL-Traffic-Management.pdf, página 1 e 2.
5.5	Deve possuir políticas de controle de acesso e autenticação baseadas nos atributos de certificado;	a) 313-F5-Using-Certificate-Authentication-in-APM.pdf, páginas 1 a 9.
5.6	Deve permitir que o WAF "recriptografe" (em SSL/TLS, utilizando um certificado interno privado diferente do certificado válido) as requisições do cliente para o servidor real, antes destas serem para ele enviadas. Deve ser possível configurar um algoritmo e tamanho de chave distinto do utilizado no estabelecimento do túnel criptografado entre o cliente e o WAF;	a) 312-F5-SSL-Methods.pdf, página 3, 4 e 5.
5.7	Implementar aceleração de TLS com instalação do certificado digital na solução, troca de chaves e criptografia dos dados assistida por hardware especializado.	a) 314-F5-Overview-of-the-hybrid-SSL-acceleration-feature.pdf, página 1.
5.8	Permitir recriptografar a conexão entre a solução e o servidor;	a) F5-311-SSL-Traffic-Management.pdf, página 1. b) 312-F5-SSL-Methods.pdf, página 3, 4 e 5.
5.9	Permitir espelhamento de tráfego de conexões TLS;	a) 315-F5-Configuring-SSL-connection-mirroring-for-Client-SSL-virtual-servers.pdf, páginas 1 e 2.
5.10	Suportar diversas cifras e protocolos SSL/TLS, incluindo TLS 1, 1.1, 1.2, 1.3, Forward Secrecy/Perfect Forward Secrecy, RSA, ECDSA, DHE, ECDHE, AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA, SHA2 (SHA256/384) e ChaCha20-Poly1305;	a) 316-F5-SSL-ciphers-supported-on-BIG-IP-platforms.pdf, páginas 1 a 19.
5.11	Em relação ao tráfego TLS, deve suportar:	a) Conforme itens abaixo
5.11.1	Autenticação do servidor pelo cliente, apresentando um certificado previamente configurado;	a) 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf, páginas 1 a 7.
5.11.2	Autenticação do cliente pela solução, através da solicitação e verificação do certificado fornecido pelo cliente;	a) 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf, páginas 1 a 7.
5.11.3	Autenticação mútua (mTLS), quando ambas as autenticações acima mencionadas ocorrendo de forma simultânea;	a) 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf, páginas 1 a 7.
5.11.4	Encaminhar ao servidor real via cabeçalho HTTP todo o certificado utilizado pelo cliente para se autenticar;	a) 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf, páginas 1 a 7.
5.11.5	Encaminhar ao servidor real via cabeçalho HTTP atributos específicos do certificado utilizado pelo cliente;	a) 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf, páginas 1 a 7.
5.11.6	Se autenticar com o servidor utilizando um certificado de cliente, próprio da solução, com os mesmos atributos do certificado do cliente;	a) 318-F5-Overview-of-the-SSL-Client-Certificate-Constrained-Delegation-feature.pdf, páginas 1 e 2.
5.11.7	As listas de acesso devem ser baseadas nos atributos de um certificado.	a) 317-F5-Configuring-the-BIG-IP-system-to-perform-two-way-SSL-authentication.pdf, páginas 1 a 7. b) https://community.f5.com/kb/technicalarticles/ssl-profiles-part-8-client-authentication/280168
5.12	Deve permitir ações caso o certificado original do servidor não seja confiável ou esteja expirado;	a) 319-F5-Overview-of-the-Server-SSL-profile.pdf, página 7.
5.13	Deve permitir "by-pass" do tráfego caso o TLS handshake falhe;	a) 320-F5-SSL-Orchestrator-SSL-Advanced-Configuration-Bypass-on-Handshake-Alert.pdf, páginas 1 e 2.
5.14	Deve permitir a verificação da validade do certificado digital apresentado:	a) 321-F5-OCSP-Authentication, páginas 1 a 8.
5.14.1	Pelo cliente através de Listas de Certificados Revogados (LCR) ou através de listas;	a) 321-F5-OCSP-Authentication, páginas 1 a 8.
5.14.2	Via OCSP (Online Certificate Status Protocol);	a) 321-F5-OCSP-Authentication, páginas 1 a 8.
5.15	Deve usar sempre o último arquivo LCR para a consulta de Lista de Certificados Revogados;	a) 321-F5-OCSP-Authentication, páginas 1 a 8.
5.16	Deve implementar os protocolos TLS versões 1.1, 1.2 e 1.3;	a) 316-F5-SSL-ciphers-supported-on-BIG-IP-platforms.pdf, páginas 1 a 19.
5.17	Deve manter e gerenciar todo o tráfego criptografado com protocolo, TLS versões 1.1, 1.2 e 1.3;	a) 316-F5-SSL-ciphers-supported-on-BIG-IP-platforms.pdf, páginas 1 a 19.
5.18	Deve implementar o algoritmo de hash SHA1;	a) 322-F5-Overview-of-BIG-IP-SSLTLS-cipher-suites.pdf, página 2.
5.19	Deve implementar renegociação de sessão;	a) 323-F5-Troubleshooting-SSLTLS-handshake-failures.pdf, página 3
5.20	Deve possuir os seguintes algoritmos de encriptação: 3DES, RSA, AES128 e AES-256, ECCDHE (P-256 e P-384) e algoritmo de autenticação ECDSA;	a) 322-Overview-of-BIG-IP-SSLTLS-cipher-suites.pdf, páginas 2 e 3.
5.21	Deve permitir geração de chaves RSA, enrollment de certificado, importação e exportação de chaves, certificados de servidores, e checagem de LCR (Lista de Certificados Revogados);	a) 324-F5-SSL-Certificate-Management.pdf, páginas 1 a 7. b) 325-F5-What-CRL-formats-does-BIG-IP-support.pdf, página 1.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
5.22	Por direcionamento inteligente de tráfego SSL entende-se a capacidade de abrir o tráfego SSL de entrada ("INBOUND") encaminhá-lo, de forma seletiva, levando em conta o contexto de serviço, às diferentes soluções de segurança que estão no ambiente de Data Center. No âmbito deste projeto serão exigidas, no mínimo, as integrações com as soluções de NG Firewall.	a) 326-F5-ssl-orchestrator-datasheet.pdf, página 3.
5.23	Deve suportar pelo menos as seguintes cifras e protocolos: TLS 1.1, 1.2 e 1.3, SHA, SHA2, AES-GCM, AES;	a) 316-F5-SSL-ciphers-supported-on-BIG-IP-platforms.pdf, páginas 1 a 19.
5.24	Deve implementar geração de chaves RSA, enrollment de certificado, importação e exportação de chaves, certificados de servidores.	a) 324-F5-SSL-Certificate-Management.pdf, páginas 1 a 7. b) 325-F5-What-CRL-formats-does-BIG-IP-support.pdf, página 1.
5.25	Deve terminar as conexões SSL com a finalidade de inspecioná-las.	a) F5-311-SSL-Traffic-Management.pdf, página 1. b) 312-F5-SSL-Methods.pdf, página 3, 4 e 5.
5.26	Deve proteger de ataques de negação de serviço que utilizem SSL.	a) 327-F5-mitigating-ddos-attacks-tech-brief.pdf, página 10.
5.27	Deve ser possível descobrir ameaças ocultas no SSL/TLS e prevenir ataques em vários estágios, usando as soluções de segurança já existentes assim como novas soluções que venham a ser adquiridas futuramente, independente de marca/modelo.	a) 326-F5-ssl-orchestrator-datasheet.pdf, páginas 1 e 2.
5.28	Deve ter capacidade de gerenciar o tráfego SSL do lado do cliente para o servidor, ou seja, deve ser capaz de decifrar todo o tráfego de entrada.	a) F5-311-SSL-Traffic-Management.pdf, página 1. b) 312-F5-SSL-Methods.pdf, página 3, 4 e 5.
5.29	Deve suportar ECDHE, RSA e DHE com suporte a Forward Secrecy.	a) 316-F5-SSL-ciphers-supported-on-BIG-IP-platforms.pdf, páginas 1 a 19. b) F5-311-SSL-Traffic-Management.pdf, página 4 e 10.
5.30	Deve suportar SSL Forward Secrecy como uma forma de melhorar a segurança nas transações SSL/TLS. Deve ser capaz de criar múltiplos Service Chains.	a) F5-311-SSL-Traffic-Management.pdf, página 4 e 10.
5.31	Deve suportar a renegociação de sessão;	a) 328-F5-Configuring-Service-Chains.pdf, páginas 1 e 2.
5.32	Deve possibilitar a monitoração e gerenciamento independente de cada dispositivo da cadeia de inspeção. Deve possuir um mecanismo de classificação contextual do tráfego que será enviado para cada dispositivo.	a) 326-F5-ssl-orchestrator-datasheet.pdf, páginas 1 e 2.
5.33	Deve fazer a monitoração dos serviços dentro da camada de inspeção	a) 329-F5-Creating-Services-Service-Chains-and-Classifer-Rules.pdf, página 4.
5.34	Deve permitir a resiliência dos serviços dentro da zona de inspeção, inclusive fazendo o balanceamento de carga entre múltiplos equipamentos do mesmo serviço.	a) 329-F5-Creating-Services-Service-Chains-and-Classifer-Rules.pdf, página 3.
5.35	Deve permitir escalar os dispositivos de segurança com alta disponibilidade, usando testes de monitoração de saúde para identificar o estado de cada equipamento de segurança.	a) 330-F5-Modify-the-F5-SSL-Orchestrator-service-monitor.pdf, página 1.
5.36	Deve ser possível prevenir ameaças de entrada (Data Center) e de saída (usuários), incluindo ataques de exploração, retorno de chamada e extração de dados.	a) 331-F5-Implementing-SSL-Forward-Proxy-on-a-Single-BIG-IP-System.pdf, página 1. b) 332-F5-Packet-Flow-in-an-SSL-Orchestrator-Reverse-Proxy.pdf, páginas 1 e 2.
6	DO GERENCIAMENTO LOCAL	a) Conforme itens abaixo
6.1	Deve possuir funcionalidade de emissão de relatório gerencial/estatístico dos acessos em ferramenta local ou remota, além do syslog ou log interno, que contenham, no mínimo:	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
6.1.1	Quantidade de acessos por VIP;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
6.1.2	Possuir MIB SNMP.	a) 334-F5-Overview-of-BIG-IP-MIB-files.pdf, página 1.
6.1.3	Quantidade de acessos por serviços e servidores;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
6.1.4	Quantidade de usuários conectados;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
6.1.5	Disponibilidade dos serviços/VIP;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
6.1.6	Tempo de latência do cliente e servidor;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
6.1.7	Throughput de requisição e resposta;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
6.1.8	Transações por segundo;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
6.1.9	Quantidade de requisições por período;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
6.1.10	7.1.10. Quantidade de sessões;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
6.1.11	7.1.11. Retenção de logs para análise posterior;	a) 333-F5-Viewing-System-Level-Statistics.pdf, páginas 1 a 8.
6.2	Deve ser disponibilizada documentação das API dos appliances que compõem a solução;	a) 335-F5-iControl-SOAP-Home, página 1. b) 336-F5-BIG-IP-AS3-API-Reference.pdf, página 1.
6.3	Deve ser capaz de analisar a performance de aplicações web.	a) 337-F5-Viewing-Application-Page-Load-Times.pdf, página 1.
6.4	Deve gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, troubleshooting, planejamento de capacidade e análise da experiência dos usuários finais no acesso às aplicações.	a) 338-F5-Troubleshooting-Applications-by-Capturing-traffic, páginas 1 e 2.
6.5	Deve, a partir das informações coletadas, permitir a análise dos dados por aplicações, por URLs, por clientes e por servidores, permitindo, assim, a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução.	a) 339-F5-Using-Local-Traffic-Policies-with-Analytics.pdf, página 1.

ITEM	DESCRIÇÃO DO ITEM	DOCUMENTO (PÁGINA)
6.6	Deve gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados. Caso a solução não possua este recurso nativamente poderá ser aceita solução de terceiros para atendimento da especificação.	a) 339-F5-Using-Local-Traffic-Policies-with-Analytics.pdf, página 1.
6.7	Deve permitir o detalhamento do tempo de resposta total de carregamento de uma URL/página.	a) 337-F5-Viewing-Application-Page-Load-Times.pdf, página 1.
6.8	Deve suportar mecanismos para criar usuários com no mínimo três conjuntos distintos de privilégios, sendo um deles somente leitura das configurações, para acesso às funções de gerenciamento dos equipamentos, via protocolos SSH, SNMP ou HTTPS.	a) 340-F5-User-roles.pdf, páginas 1 a 5.
6.9	Deve possibilitar a coleta de dados de gerenciamento dos equipamentos utilizando os protocolos SNMPv2c e SNMPv3.	a) 341-Monitoring-BIG-IP-System-Traffic-with-SNMP, páginas 1 e 2.
6.10	Deve suportar MIB SNMP.	a) 334-F5-Overview-of-BIG-IP-MIB-files.pdf, página 1.
6.11	Deve permitir a configuração de endereços IPs para o envio de traps SNMP (alarmes).	a) 295-F5-Configuring-SNMP-Traps.pdf, página 1 a 4.



Conecte o presente, **proteja o futuro.**

obrigado!