JUSTIÇA FEDERAL DA 3ª REGIÃO
TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO
Secretaria de Tecnologia da Informação - SETI
Divisão de Infraestrutura e Conectividade - DINC

Estudo Técnico Preliminar para contratação de solução de Firewall de Nova Geração (NGFW)

HISTÓRICO DE REVISÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
04/03/2024	1.0	Criação Documento	Bryan
21/03/2024	1.1	Revisão e atualização	Elias
25/03/2024	1.2	Revisão e atualização	Elias
26/03/2024	1.3	Revisão e atualização	Bryan
05/06/2024	1.4	Alteração de requisitos solicitados pela JFSC	Guilherme
31/08/2024	1.5	Revisão	Leonardo
20/09/2024	1.6	Revisão	Guilherme
24/09/2024	1.7	Ajuste	Flávio

INTRODUÇÃO

O Estudo Técnico Preliminar - ETP tem por objetivo identificar e analisar os cenários para o atendimento a demanda da Administração de contratar uma nova solução de firewall de próxima geração (*Next-Generation Firewall - NGFW*, em inglês), bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1. Identificação das necessidades de negócio:

No cenário atual do Tribunal Regional Federal 3ª Região, as atividades judicante e administrativa são amparadas fortemente no uso de soluções de TI - equipamentos, softwares e sistemas de informação - que se tornaram vitais para o funcionamento e melhoria dos serviços prestados ao jurisdicionado. Como consequência, a proteção do ambiente tornou-se fator essencial para manutenção da disponibilidade, confidencialidade e integridade dos serviços de TI e do funcionamento do Tribunal, bem como para manutenção da confidencialidade, integridade, disponibilidade e autenticidade dos dados.

A utilização de recursos e soluções de Tecnologia de Informação tanto nesse tribunal quanto nos demais trouxeram uma mudança extremamente significativa nos processos internos e interação com seu público. Essas alterações promoveram, e ainda promovem, celeridade dos resultados e aumento de produtividade das atividades jurisdicionais, assim como ampliou e melhorou o acesso à Justiça. Atualmente são disponibilizados através da rede mundial de computadores, tanto para o público interno como externo, diversos sistemas e serviços acessíveis por dispositivos como computadores e dispositivos móveis.

Por conseguinte, a expansão da utilização da Internet com a interconexão de instituições, corporações e pessoas, e o tráfego imenso de informações na rede provocou o interesse de pessoas mal-intencionadas visando à obtenção de vantagens financeiras, coleta de informações confidenciais, prática de vandalismo e golpes, realização de ataques ou a mera disseminação de mensagens indesejadas ou informação falsas.

As formas de ataques, especialmente os vindos da internet, tornam-se cada vez mais sofisticadas e a cada dia novos tipos de ataques são desenvolvidos e novas vulnerabilidades são exploradas. É importante, portanto, implantar métodos de segurança que possam auxiliar na tentativa de proteção dos dados e a segurança da informação de forma dinâmica.

Vale ressaltar que um bom método de segurança é garantir que os recursos tecnológicos de segurança estejam bem alocados dentro da infraestrutura e que estejam funcionando a contento. Não obstante, a busca por redução de complexidade nos itens supracitados se torna cada vez mais necessária devido à grande quantidade de ferramentas e serviços disponibilizados pelas soluções de segurança. Além disso, também é interessante buscar a facilitação da gerência da solução. Uma arquitetura robusta, porém, mais simplificada, auxilia na disponibilidade de todos os serviços prestados.

Dito isso, verificamos que a solução atual utilizada por esse Tribunal deixa de atender principalmente o requisito de simplificação do ambiente. Além disso, o modelo de equipamento já está em fim de vida como foi anunciado pelo fabricante e, atualmente, permite apenas a renovação do contrato de serviço até 31 janeiro de 2027, assim como as atualizações de software e vacinas[1]. Portanto, é necessária a aquisição de uma nova solução, aproveitando para superar dificuldades da arquitetura diferente atual. Uma solução sem suporte ou atualizações se torna ineficaz e pode

[1] https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/firepower-4110-series-security-appliances-eol.html

trazer grandes prejuízos tanto à instituição quanto à população que utiliza os serviços fornecidos por este tribunal. Por fim, a solução atual não suporta algumas necessidades modernas em camada sete (aplicação) em que *wildcards* (asteriscos) deveriam ser aplicados em regras.

Ressalta-se, também, o ciclo de vida do ativo, em que segundo RESOLUÇÃO Nº CJF-RES-2018/00477, Art 3º § 1º, o prazo mínimo de garantia para ativos de rede é de 5 anos. Entende-se que um Firewall pode ser considerado um equipamento de segurança, no qual é definido um prazo de garantia de 4 anos, porém, por ter um comportamento para operação de rede, a área técnica entende que sua classificação mais adequada é como ativo de rede, pois seu ciclo de vida no fabricante é idêntico ao ciclo de vida de um switch, por exemplo.

Diante do exposto, e, considerando-se (a) as restrições de espaço físico na sala de computadores (Data Center), (b) a necessidade de implementação de práticas sustentáveis nas contratações públicas através da aquisição de produtos de menor impacto ambiental, com maior durabilidade, menor consumo de energia e materiais, (c) a necessidade de implementar a totalidade de recursos de segurança que permitam gerenciamento centralizado, simplificado e com facilidade de configuração e operação, não foram consideradas as soluções de mercado que atendem ou implementem apenas um conjunto específico e limitado de recursos, isto é, soluções pontuais aplicáveis para cada tipo de ameaça existente, como web gateway, firewall tradicional (hardware e/ou software), equipamentos de IDS/IPS (prevenção e detecção de ameaças), equipamentos de filtragem de conteúdo, DNS e aplicação (WAF), etc.

Da mesma forma, as soluções baseadas exclusivamente em software, livre ou pago, não foram consideradas uma vez que (a) necessitam de investimento em infraestrutura (aquisição de equipamentos, sistemas operacionais, etc), (b) exigem também, no caso de software pago, a manutenção de contratos de subscrição para atualização de software e das bibliotecas de assinatura de código malicioso, quando contemplam esta funcionalidade, (c) exigem, no caso de software livre, a designação

de equipe de segurança dedicada e especializada e investimentos em processos contínuos de capacitação, (d) impõem restrições à alta disponibilidade e à prestação de suporte adequado e tempestivo, (e) além de não implementarem todos os requisitos de segurança de porte corporativo, de forma ampla e efetiva.

Por sua vez, também não foram consideradas soluções oferecidas como serviço, visto que promovem a transferência de domínio dos recursos de segurança a terceiros e é competência da administração a salvaguarda dos ativos de informação. Abordaremos em mais detalhes mais adiante, neste mesmo documento.

Isto posto, foram consideradas as soluções integradas de segurança de redes em formato de appliance, isto é, hardware e/ou software projetados e dimensionados especificamente para analisar e suportar um grande volume de tráfego e que permitam a implementação de diversos recursos de segurança. Diferentemente dos firewalls convencionais, esses equipamentos de segurança com característica de Next Generation Firewall (Firewall de nova geração) ou Unified Threat Management (Gerenciamento Centralizado de Ameaças) são capazes também de realizar reconhecimento de aplicações e de usuários, auxiliar na prevenção de ameaças e no controle de permissões e políticas de acesso com maior granularidade. Dado o risco da exposição indevida de informações ou de ataques que reduzam a disponibilidade de sistemas, esses equipamentos permitem ainda a possibilidade de verificação do comportamento do tráfego em tempo real, identificando acessos abusivos ou indevidos.

Identificação das necessidades tecnológicas:

- **Requisitos de Negócio:**

A presente contratação orienta-se pelos requisitos de negócio descritos no item 1.1 deste presente documento.

- **Requisitos de Capacitação:**

O treinamento oficial para a equipe técnica da JF3R é essencial para garantir a competência e atualização dos profissionais diante das constantes evoluções tecnológicas e das ameaças cibernéticas em constante mutação. A capacitação oficial proporciona conhecimentos específicos e práticos, permitindo uma resposta eficaz a incidentes e a implementação adequada de medidas de segurança, maximizando a eficiência operacional e a proteção dos sistemas e dados do tribunal.

O treinamento oficial da fabricante deverá conter as seguintes características mínimas:

- Objetivo: Implantação, configuração, operação e gerenciamento da solução.
- Conteúdo: Arquitetura da solução, componentes, rotinas de administração e análise básica de problemas (troubleshooting).
- Participantes: A área técnica é composta por 5 servidores. Este é o número mínimo de participantes no treinamento. Porém, a subsecretaria UARI solicitou registrar preço para participantes adicionais, contemplando a DINC (1), UISI(1), SETI (1), eventual posse de novos servidores (2). Portanto, iremos registrar preço do treinamento na solução para um total de 10 participantes.
- Carga horária mínima: 40 (quarenta) horas.
- Modalidade: Preferencialmente remoto em simulador virtual com as características idênticas à solução adquirida.
- Material Didático: A CONTRATADA deverá fornecer todo o material didático de apoio necessário para o treinamento devendo entregar material expositivo e bibliografia referente ao curso ministrado. O material em formato digital e deverá ser ofertado em língua portuguesa (preferencialmente) ou inglesa.
- A prestação dos serviços de treinamentos deverá ocorrer em dias úteis, preferencialmente, no horário compreendido entre 09:00 e 18:00. A carga horária total (40h) será distribuída a critério da CONTRATANTE, podendo o treinamento ser

segmentado em mais de uma semana, com uma carga horária menor. O motivo desse aspecto é a alocação da equipe para o treinamento e conciliação das atividades rotineiras.

- Certificado: Deverá ser emitido certificado de conclusão do curso, em formato virtual, que contenha, no mínimo, nome completo do participante, nome da instituição de treinamento, carga horária, data de início e término, conteúdo programático, assinatura do responsável pelo treinamento.
- Qualificação do Instrutor: O instrutor deverá ser certificado pelo fabricante na solução ofertada. Justificativa: o instrutor certificado garante um nível de conhecimento e habilidade na área que está lecionando, auxiliando na transmissão do conhecimento técnico, garantindo que os participantes recebam instruções de qualidade e informações atualizadas em conformidade com as melhores práticas do fabricante.
- Todas as despesas necessárias à prestação dos serviços incluindo deslocamento e hospedagem do instrutor serão de exclusiva responsabilidade da CONTRATADA.
- Justificativa: O treinamento oficial da fabricante garante aderência do conteúdo do treinamento às funcionalidades dos equipamentos da solução contratada, pois haverá respaldo da própria fabricante na sua elaboração, garantindo conformidade ao que será adquirido pela CONTRATANTE.
- Quantidade de participantes dos demais órgãos atendendo suas próprias necessidades :
  - TRF2 = 4 servidores
  - SJES = 4 servidores
  - TRF4 = 5 servidores
  - SJSC = 3 servidores
  - SJRS = 6 servidores
  - TRF1 = 6 servidores
  - SJDF = 4 servidores .

- **Requisitos de Manutenção:**

O equipamento deverá ter os principais componentes (módulos, PSU, transceivers e chassi) substituíveis.

Os serviços de manutenção corretiva deverão ser executados onde o equipamento encontrar-se instalado (on-site).

Durante o período de garantia, a parte ou peça defeituosa deverá ser substituída sem ônus para o Contratante.

As peças substituídas deverão ser novas, idênticas às originais ou de qualidade superior, homologadas pelo fabricante.

Na data da proposta, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de *end-of-sale.*

O equipamento deverá ser atualizável durante todo ciclo de garantia (60 meses), não podendo entrar em *end-of-life* ou *extended support* nesse período.

As atualizações de firmware deverão envolver correções de falhas (bugs), correções de segurança e melhorias (evolutivas A CONTRATADA deve fornecer atualizações de firmware e/ou software de acordo com as recomendações do Fabricante dos equipamentos, garantindo que estes estejam protegidos contra as ameaças mais recentes e que possuam os recursos e funcionalidades mais atualizados. As atualizações devem ser aplicadas sem causar impacto significativo na operação dos sistemas e com o mínimo de interrupções no acesso aos serviços.

A CONTRATADA deve garantir a disponibilidade contínua dos equipamentos de segurança da informação, minimizando o tempo de inatividade e as interrupções no funcionamento dos sistemas. O suporte técnico deve ser capaz de oferecer soluções rápidas e eficazes para restaurar a operacionalidade dos equipamentos em caso de falhas ou problemas.

A CONTRATADA deve cumprir os prazos previstos no item “Níveis de Serviço” deste documento, para o atendimento e resolução de problemas relatados pela Justiça Federal da 3ª Região - JF3R.

Fornecimento de serviços de manutenção e assistência técnica: a CONTRATADA será responsável por oferecer serviços de manutenção e assistência técnica dos bens durante o período de garantia através de mão-de-obra própria ou através de mão-de-obra do FABRICANTE. Quando necessário deslocamento físico o tempo de deslocamento do técnico **será contabilizado no prazo de resolução da solução**, Como atividades que requerem deslocamento entendem-se quaisquer atividades que possa causar perda de comunicação externa (perda de comunicação remota com a infraestrutura da JF3R e/ou atividade crítica que possa gerar esse cenário) e/ou troca de peças defeituosas “in loco” pela Contratada.

- **Requisitos Temporais:**

O prazo de vigência da contratação será de, no máximo, 5 (cinco) anos, 5 (cinco) meses e 11 (onze) dias contados da assinatura do termo de contrato, sendo:

EVENTO	PRAZO MÁXIMO PREVISTO (DIAS CORRIDOS)
Reunião inicial + Ata Definitiva	C + 7
Entrega do Plano de Projeto	C + 15
Entrega dos equipamentos	C + 60
Recebimento Provisório dos equipamentos	C + 70
Recebimento Definitivo dos equipamentos	C + 80
Instalação física da solução, configuração e integração, testes e operação assistida	C + 140
Ativação de licenças	C + 141
Treinamento	C + 150
Recebimento Provisório dos serviços de implantação	C + 150
Recebimento Provisório da ativação de licenças	C + 151
Entrega de documentação de implantação	C + 155
Recebimento Provisório dos serviços de treinamento	C + 160

Recebimento Definitivo da ativação de licenças	C + 161
Início da garantia dos bens e serviços	C + 161
Recebimento Definitivo dos serviços de implantação	C + 165
Recebimento Definitivo dos serviços de treinamento	C + 170
Recebimento Definitivo dos serviços de operação e sustentação	C + 1940
Recebimento Definitivo do suporte técnico, atualizações e garantia	C + 1961

TABELA 1

EVENTO	DESCRIÇÃO DO EVENTO	PRAZO MÁXIMO PREVISTO (DIAS CORRIDOS)
1	Assinatura do Contrato	C (data da assinatura do contrato)
2	Reunião Inicial + Ata definitiva	C + 7
3	Entrega do Plano de Projeto	C + 15
4	Entrega dos equipamentos	C + 60
5	Recebimento Provisório dos equipamentos	EVENTO 4 + 10
6	Recebimento Definitivo dos equipamentos	EVENTO 5 + 10
7	Instalação física da solução, configuração e integração, testes e operação assistida	EVENTO 6 + 60
8	Ativação de licenças	EVENTO 7 + 1
9	Treinamento	C + 150
10	Recebimento Provisório dos serviços de implantação	EVENTO 7 + 10
11	Recebimento Provisório da ativação de licenças	EVENTO 8 + 10
12	Entrega de documentação de implantação	EVENTO 7 + 15
13	Recebimento Provisório dos serviços de treinamento	EVENTO 9 + 10
14	Recebimento Definitivo da ativação de licenças	EVENTO 11 + 10
15	Início da garantia dos bens e serviços	EVENTO 11 +10
16	Recebimento Definitivo dos serviços de implantação	EVENTO 12 + 10
17	Recebimento Definitivo dos serviços de treinamento	EVENTO 13 + 10
18	Recebimento Definitivo dos serviços de operação e sustentação	EVENTO 7 + 1800
19	Recebimento Definitivo dos serviços de suporte técnico, atualizações e garantia	EVENTO 15 + 1800

TABELA 2

Os eventos apresentados poderão ser executados, se possível, em ordem antecipada, porém mantendo-se os prazos máximos previsto em cronograma. A dependência somente em relação ao prazo de assinatura do Contrato permite a antecipação de atividades, mitigando burocracias temporais. Por exemplo, um

treinamento poderá ocorrer antes da entrega de um equipamento. Destaca-se, contudo, que os prazos máximos previstos não são alterados.

Os eventos que possuem dependência com outros eventos não possuem flexibilidade.

Os prazos são contados em dias corridos. Caso o término ocorra em fim de semana ou feriado, valerá o próximo dia útil subsequente.

Considerando que se trata de ATA de Registro de Preços, certos eventos poderão gerar contratações em separado e, portanto, com suas próprias vigências particulares.

- **Requisitos de Segurança e Privacidade:**

A CONTRATADA deverá observar integralmente os requisitos de Segurança da Informação e Privacidade (SIP) descritos a seguir, conforme princípios e procedimentos elencados na Política de Segurança da Informação da CONTRATANTE, devendo:

- Garantir a interoperabilidade e compatibilidade da solução com os equipamentos existentes no data center da CONTRATANTE;
- Observar as diretrizes de SIP conforme Seção 7 do Anexo I da IN SGD/ME nº 94/2022 e a legislação vigente;
- Assegurar a operacionalidade contínua e eficiente da solução de TIC;
- Implementar medidas robustas para prevenir vazamentos de dados e fraudes digitais;
- Definir e manter um processo de gestão de riscos de SIP que envolva a solução de TIC;
- Facilitar a auditoria de SIP através de trilhas de auditoria detalhadas e rastreabilidade;
- Implementar estratégias para assegurar a continuidade das operações de TIC;

- Manter conformidade com a Lei nº 13.709/2018 (LGPD) e legislação vigente para dados pessoais e informações classificadas;
- Submeter-se a auditorias periódicas para verificar a aderência aos requisitos de SIP;
- Gerenciar e tratar incidentes de SIP de forma sistematizada;
- Implementar diretrizes para o desenvolvimento e obtenção de software seguro;
- Contemplar processos de gestão de mudanças e capacidade;
- Implementar controles criptográficos.

A CONTRATANTE realizará acompanhamento contínuo e revisões periódicas dos requisitos e obrigações de SIP.

- **Requisitos da Arquitetura Tecnológica:**

A CONTRATADA deverá garantir a completa interoperabilidade e compatibilidade entre a solução adquirida no presente documento e os principais equipamentos de redes (switches de data center e roteadores) presentes no Data Center da CONTRATANTE. Os fabricantes são Cisco, Juniper, HP e Dell e não estão em end-of-life.

Na Figura 1, abaixo, temos a visão lógica da nova solução de Firewall:

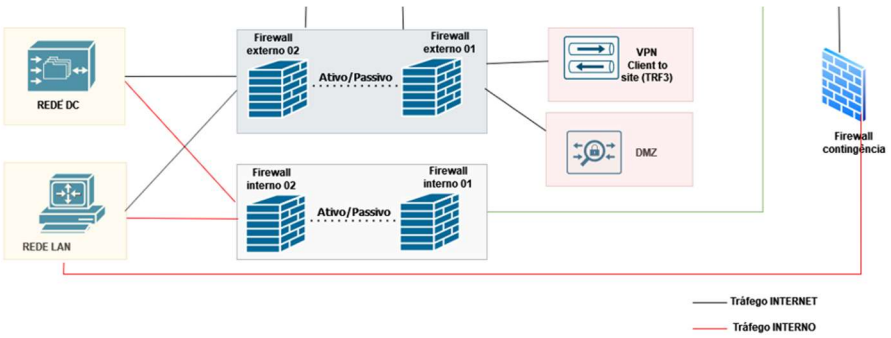

FIGURA 1- ESCOPO DA CONTRATAÇÃO COM FIREWALL EXTERNO (2), FIREWALL INTERNO (2) E FIREWALL DE CONTINGÊNCIA (1)

A seguir, a Figura 2 detalha um pouco mais o objetivo a ser alcançado, desenhando as conexões físicas:

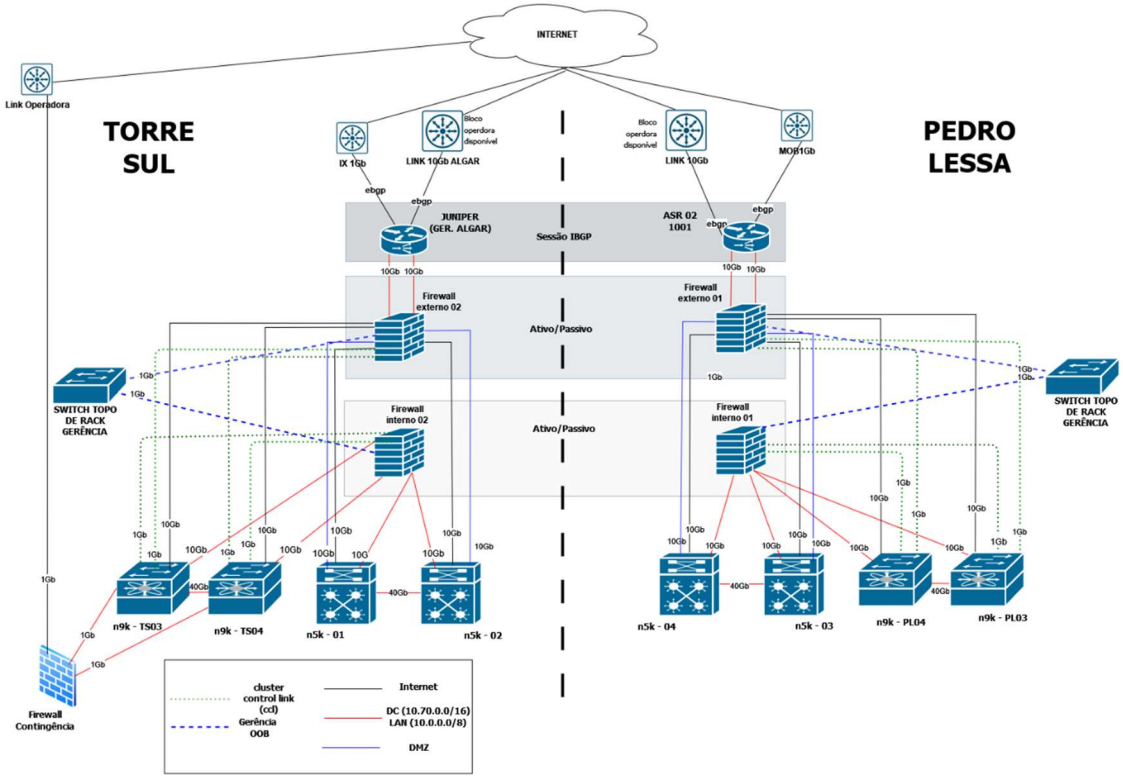

FIGURA 2 - MAPA DETALHADO DA SOLUÇÃO PRETENDIDA (VISÃO FÍSICA)

Por uma questão de simplificação do desenho, o firewall de contingência não foi desenhado no datacenter secundário (Pedro Lessa), mas como ele será um espelho do datacenter primário (Torre Sul), haverá um segundo firewall de contingência conectado a um link de Internet independente no site Pedro Lessa.

Características Gerais

A solução principal deve ser composta por 4 (quatro) *appliances* físicos para prover alta disponibilidade. Adicionalmente, haverá um (1) appliance *standalone* físico por site, para uso em caso de emergência. A Figura 1 apresenta esses equipamentos com os nomes Firewall interno 01 e 02, Firewall externo 01 e 02 e Firewall Contingência.

Abaixo teremos as características dos 4 *appliances* principais e suas funcionalidades.

Ao final, serão descritas as características do firewall de contingência.

Solução principal

Cada par de firewall deverá ser idêntico entre si em suas características físicas.

Cada appliance de firewall deve ser fornecido através de módulos e/ou nativamente:

- Opção 1:
  - 16 portas 10 GE SFP+
  - 4 portas 25 GE SFP28;
  - 8 transceivers SFP+ RJ45 10 GE
  - 8 transceivers SFP+ 10 GE SR (Short Range) Multimodo;
  - 4 transceivers SFP28 25 GE SR (Short Range) Multimodo;
  - 1 porta RJ45 1 GE dedicada para gerenciamento;
  - Portas redundantes para sincronismo do cluster.
- Opção 2:
  - 8 portas 10 GE RJ45;
  - 8 portas 10 GE SFP+;
  - 4 portas 25 GE SFP28;
  - 8 transceivers SFP+ 10 GE SR (Short Range) Multimodo;
  - 4 transceivers SFP28 25 GE SR (Short Range) Multimodo;
  - 1 Porta RJ45 1 GE dedicada para gerenciamento;
  - Portas redundantes para sincronismo do cluster.

Em ambos os casos, as interfaces deverão ser fornecidas com todos os conectores, cabos, e demais componentes que se façam necessários para o devido uso.

Cada appliance deve possuir interfaces de rede redundantes e dedicadas para sincronismo;

As soluções devem suportar agregação de link (LACP 802.3ad).

Cada appliance da solução firewall (interna e externa) NGFW deve suportar, no mínimo, os seguintes requisitos:

- NGFW Throughput de 33 Gbps com funcionalidades de firewall, controle de aplicação, IPS ativas e logging ativos.
- Threat Protection Throughput de 28.5 Gbps com funcionalidades de Firewall, controle de aplicação, URL Filtering, IPS, Antivirus/antimalware e logging ativos.
- IPSec VPN Thoughtput de 20 Gbps com testes usando chaves AES256-SHA256 ou AES-GCM. Para chaves de menor complexidade (i.e. AES128, SHA1, SHA128) solicita-se um throughput de 40 Gbps.
- SSL VPN Thoughtput de 8 Gbps com RSA 2048 ou AES128. Caso o datesheet do equipamento não comprove tráfego SSL VPN e SSL IPSec separadamente, considera-se o tráfego 28 Gbps para o item 4.8.5.7.3 ou 48 Gbps para chaves de menor complexidade.
- Cada appliance deve suportar, no mínimo, 7.000.000 (sete milhões) de conexões e, no mínimo, 350.000 (duzentos mil) conexões simultâneas por segundo.

Os *Throughputs* e as interfaces solicitados neste item deverão ser comprovados através de *datasheet* disponibilizado pela fabricante, preferencialmente, de acesso público, na Internet, assim como, posteriormente, na fase de testes.

Em caso de uso em cluster, ele deverá operar em modo *active-standby* (ativo-passivo) sem a necessidade de licença adicional. Em complemento, cada nó do cluster, isoladamente, deve atender toda a carga de todos os data centers da CONTRATANTE.

Em caso de indisponibilidade do nó ativo do cluster, a solução deverá ter RTO igual à zero (RTO=0) no chaveamento das operações para o nó passivo.

A configuração dos nós deverá ser realizada de forma centralizada, de modo que não seja necessário replicar manualmente configurações entre eles, exceto as configurações específicas de cada equipamento.

A solução deverá contar uma gerência centralizada para realizar as atividades supracitadas.

Deve possuir dispositivos de armazenamento configurados de maneira redundante (RAID1 ou similar) e distribuídos entre dispositivos para armazenamento do sistema e dispositivos para armazenamento de log.

Os dispositivos de armazenamento de dados de sistemas devem usar tecnologia de armazenamento rápido (SSD ou similar) com volumetria mínima de 200 GB útil.

Os dispositivos de armazenamento de logs podem utilizar tecnologia de armazenamento rápido (SSD ou similar) ou discos mecânicos com volumetria mínima de 500 GB útil.

Serão aceitos sistemas em que haja somente um par de dispositivos de armazenamento para Sistema Operacional e Logs, porém somente serão aceitos se utilizaram tecnologia de armazenamento rápido (SSD) e que a volumetria seja a soma dos valores acima, ou seja, 700 GB útil.

Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 110 e 240 VAC que permitam hot-swap. Preferencialmente, utilizar padrão de conexão C13/C14.

Deve possuir ventiladores redundantes

Solução Principal - Políticas de Firewall

Deve realizar controles de políticas por porta e protocolo.

Deve realizar controles de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características) e categorias de aplicações.

Deve realizar controle de políticas por usuários, grupos de usuários, IPs e subredes IPv4.

Deve possibilitar a utilização de *wildcard* nos controles de políticas, como, por exemplo, os casos a seguir:

- *exemplo.com
- *.exemplo.com
- *.subdominio.exemplo.com

A solução deve permitir a configuração de políticas que utilizem o posicionamento geográfico ou código dos países ou grupos de endereços IP dos países de origem e destino do tráfego.

Deve realizar controle, inspeção e descriptografia de SSL por política para tráfego de entrada (*inbound*) e saída (*outbound*).

Deve realizar *offload* de certificado em inspeção de conexões SSL de entrada (*Inbound*);

Deve descriptografar tráfego *inbound* e *outbound* em conexões negociadas com HTTP/2, TLS 1.2 e 1.3;

Deve permitir espelhar tráfego descriptografado pelo *firewall* em uma de suas interfaces de rede permitindo integração com soluções Forense;

Deve permitir bloqueios por tipo de arquivo;

Deve oferecer suporte a objetos e regras *multicast*.

Deve permitir agendamento de políticas, de modo a habilitar e desabilitar políticas em horários e datas pré-definidos automaticamente.

Deverá ter integração com o Cisco ISE para identificação de usuários e criação de regras com esses usuários identificados.

Suportar a criação de políticas por “geolocalização”, permitindo que configuração de ações (como liberação e bloqueio) para o tráfego de um ou mais países.

Deve possibilitar a identificação dos países de origem e destino nos logs dos acessos.

Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

Solução Principal – Qualidade de Serviço (QoS - Quality of Service)

Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, requer que a solução, além de poder permitir ou negar esses tipos de aplicações, a solução deve ter a capacidade de controlá-las por políticas de máximo de largura de banda, quando forem solicitadas por diferentes usuários ou aplicações.

Deve realizar *traffic shaping* e *QoS* baseado em políticas.

Suportar a criação de políticas de *QoS* por:

- Endereço de origem;
- Endereço de destino;
- Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e redes sociais.
- O traffic shapping e o QoS deve possibilitar a definição de classes por:
- Banda garantida;
- Banda máxima;
- Fila de prioridade;
- Suportar priorização RealTime de protocolos de voz e vídeo;
- Suportar marcação de pacotes Diffserv;
- Disponibilizar estatísticas RealTime para classes de QoS;
- Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

Solução Principal –*VPN IPSec*

Funcionalidade de VPN deve ser licenciada para funcionamento em cluster ativo-passivo.

Deve incluir suporte a IPSEC manual, IKEv1 e IKEv2.

Deve suportar criptografia simétrica AES-128 e AES-256.

Deve suportar criptografia assimétrica Diffie-Hellman: Grupo 14 até Grupo 20.

Deve suportar, pelo menos, integridade de dados sha1, sha-256 e sha-512.

Deve incluir suporte para *VPN site-to-site* nas seguintes topologias: *Full Meshed* (todos para todos), Estrela (escritórios remotos para site central), *Hub and Spoke* (site remoto através de site central para outro site remoto).

Deve incluir gerenciamento centralizado de *VPNs*, com a possibilidade de criar várias *VPNs* ao mesmo tempo, sem a necessidade de efetuar esta tarefa por meio de linha de comando (*CLI*).

Deve permitir que o administrador aplique regras de segurança para controlar o tráfego dentro da VPN.

Deve suportar *VPNs* usando, pelo menos, roteamento estático, BGP e OSPF.

Deve incluir um mecanismo para mitigar o impacto de um ataque *DoS* ao IKE, fazendo a distinção entre *peers* conhecidos e desconhecidos.

Deve incluir a funcionalidade para estabelecer *VPNs* com *gateways* com IPs públicos e dinâmicos.

O equipamento deve permitir, no mínimo, 500 (quinhentas) VPNs site-to-site.

Permitir criação de VPN nos modos “policy-base” e “routed-based”.

Solução Principal - SSL VPN

Dever permitir e estar licenciado para, no mínimo, 1000 (mil) usuários concorrentes, acessando a partir de qualquer dispositivo, incluindo dispositivos móveis. O equipamento deverá ser escalável para, pelo menos, 3000 (três mil) usuários concorrentes.

Deve possuir o modo "*Portal*", 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.

Deve possuir o modo "*Network*", onde um usuário se conecta efetivamente à rede interna, obtendo um endereço *IP* roteável pela rede interna.

Deve possuir suporte a *split tunneling*.

Deve possibilitar a customização da interface gráfica da página de *Login* e mensagens de apresentação ao usuário.

Deve oferecer acesso remoto seguro à rede inteira para qualquer aplicação baseada em IP (TCP ou UDP).

Suporte a *Single-Sign-On* (*SSO*): deve ser capaz de realizar *SSO* utilizando Kerberos ou qualquer protocolo similar.

Deverá implementar suporte à validação da estação do usuário para, no mínimo, os seguintes recursos:

- Versão do Sistema Operacional;
- Firewall ativado;
- Antivírus instalado;
- Deverá ser possível configurar uma ação dependendo da validação da estação do usuário.

A configuração dessas ações deverá ser através de interface gráfica.

Deverá permitir conferência do endereço IP quanto à origem Geográfica.

Deverá ser capaz de autenticar usuários suportando os seguintes esquemas: Base de Dados do próprio sistema, Base de dados *LDAP*, RADIUS, Active Directory, Office 365 (Azure AD) e Certificado Digital padrão X.509, incluindo os certificados emitidos pelo ICP-Brasil.

Suportar autenticação de múltiplos fatores.

Deve permitir a autenticação em, pelo menos, 5 diferentes domínios do Active Directory simultaneamente.

Os clientes devem estar disponíveis para estações de trabalho e dispositivos móveis (*smartphones*, *tablets*, entre outros) nos principais sistemas operacionais (Android e iOS), em suas últimas versões, não implicando em custo adicional para a contratante.

Deverá haver, pelo menos, uma opção de cliente que não utilize Java.

Solução Principal – Proteção de Ameaças e Sistema de Prevenção e Identificação de Intrusão (IPS/IDS)

As funcionalidades de bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware) deverão estar presentes na solução;

Deve sincronizar as assinaturas de IPS, antivírus, *antispyware* quando implementado em alta disponibilidade e ativo/passivo;

As funcionalidades de IDS/IPS e Firewall devem ser implementadas em um mesmo *appliance*, sendo que a comunicação entre eles deverá ser interna, sem a necessidade de uso de quaisquer interfaces externas.

Deve incluir pelo menos os seguintes mecanismos de detecção:

- Assinaturas de vulnerabilidades e exploits;
- Assinaturas de ataque;
- Validação de protocolo;
- Detecção de anomalia;
- Detecção baseada em comportamento.

O administrador deve ser capaz de configurar a inspeção somente para tráfego entrante (*inbound*).

O *IPS* deve incluir definições de ataques que protejam tanto clientes quanto servidores.

O *IPS* deve oferecer políticas predefinidas.

O *IPS* deve incluir a habilidade de interromper temporariamente as proteções para fins de troubleshooting.

O mecanismo de inspeção deve ser capaz de receber e implementar, em tempo real, atualizações para os ataques emergentes sem a necessidade de reiniciar o *appliance*.

O sistema deverá permitir a atualização periódica (agendamento) das assinaturas por meio de conexão segura.

O administrador deve ser capaz de ativar novas proteções baseado em parâmetros configuráveis (indicador de impacto na performance, severidade da ameaça, proteção dos clientes, proteção dos servidores).

A solução deve ser capaz de detectar e prevenir pelo menos as seguintes ameaças:

- Exploits e vulnerabilidades específicas de clientes e servidores;
- Mau uso de protocolos, isto é, fora do padrão da RFC;
- Comunicação outbound de malware;
- Tentativas de tunneling;
- Tráfego de aplicações indesejadas, incluindo IM e P2P;
- Ataques genéricos sem assinaturas predefinidas.

Deve oferecer proteções contra aplicações específicas como *peer-to-peer*, com a opção de bloquear estas aplicações.

Para cada proteção devem estar inclusos: a descrição da vulnerabilidade, a descrição da ameaça e a severidade da ameaça.

Deve incluir a opção de adicionar exceções baseado na fonte ou destino, ou combinação de ambos.

A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de *e-mail*, *DNS*, *FTP*, serviços Windows (*Microsoft Networking*) e *VoIP*.

A solução deve suportar a ativação de assinaturas apenas em modo de monitoração.

A solução deve permitir o bloqueio de "*exploits*" conhecidos.

A solução deverá possuir mecanismo de proteção contra-ataques de *phishing*.

A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

A solução deve prover proteção contra-ataques de negação de serviços.

A solução deve ser capaz de detectar e bloquear ataques conhecidos e desconhecidos heuristicamente.

A solução deve incluir proteção aos protocolos POP e SMTP.

A solução deve permitir a configuração de inspeção do IPS baseado em políticas que utilizem o posicionamento geográfico de origens/destinos do tráfego.

A solução deve permitir a inspeção de tráfego sobre o protocolo HTTPS (*inbound/outbound*).

Deve oferecer a opção de bloquear controles *ActiveX* e *applets* Java que possam comprometer usuários *web*.

Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades em diversas áreas de interesse do administrador e a evolução no tempo. As diferentes áreas de interesse devem ser definidas usando filtros customizáveis para selecionar alertas baseados em qualquer propriedade ou combinação de propriedades do mesmo, incluindo pelo menos: origem, destino, serviço, tipo e nome do alerta.

Deve possibilitar a criação de assinaturas customizadas pela interface gráfica do produto ou importar assinaturas no formato SNORT.

O sistema deverá implementar mecanismo de resolução de endereços via DNS (ou seja, implementar o comportamento de “DNS resolver”), para que conexões com destino a domínios maliciosos sejam resolvidas pelo componente “firewall” com endereços previamente definidos.

Solução Principal – Controle de Aplicações

Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

Reconhecer aplicações relacionadas a tráfego *peer-to-peer*, redes sociais, acesso remoto, *update* de software, protocolos de rede, *VoIP*, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

Reconhecer, pelo menos, 5500 aplicações comprovadas por documentação online ou no próprio equipamento. As seguintes aplicações devem ser identificadas, não se limitando a elas: BITTORRENT, SKYPE, FACEBOOK, LINKED-IN, TWITTER (X), LOGMEIN, TEAMVIEWER, MS-RDP, VNC, GMAIL, YOUTUBE, HTTP-PROXY, HTTP-TUNNEL, FACEBOOK CHAT, GMAIL CHAT, WHATSAPP, 4SHARED, DROPBOX, GOOGLE DRIVE, ONEDRIVE, DB2, MYSQL, ORACLE, ACTIVE DIRECTORY, KERBEROS, LDAP, RADIUS, ITUNES, DHCP, FTP, DNS, WINS, MSRPC, NTP, SNMP, RPC OVER HTTP, GOOGLE-DOCSDeve inspecionar o *payload* do pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pela fabricante independente de porta e protocolo.

Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado.

Identificar o uso de táticas evasivas, inclusive via comunicações criptografadas.

Para tráfego criptografado (SSL), deve descriptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pela fabricante.

Atualizar a base de assinaturas de aplicações automaticamente.

Reconhecer aplicações em IPv6.

Limitar a banda (*download/upload*) usada por aplicações (*traffic shaping*), baseado em IP.

Capacidade de identificar o usuário que acessa a aplicação através de integração ao *Microsoft Active Directory e/ou Office 365* (Azure AD), sem a necessidade de instalação de agente em *Domain Controller*, nem nas estações dos usuários.

Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

Deve suportar múltiplos métodos de identificação e classificação das aplicações. Pelo menos, deverão possuir checagem de assinaturas, decodificação de protocolos e análise heurística.

Permitir a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução ou por meio de solicitação à fabricante. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares e contexto (sessões ou transações).

A solução deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

A solução deve permitir alertar o usuário quando uma aplicação foi bloqueada.

Solução Principal – Identificação de Usuários

Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, *Active Directory* e base de dados local.

Deve implementar mecanismo de integração com o serviço de diretório AD para identificação de usuários e de grupos de usuários, permitindo maior

granularidade por meio de controles e de políticas baseadas em usuários e grupos de usuários.

Deve permitir a utilização de, pelo menos, 3 diferentes domínios do Active Directory simultaneamente.

Deve possuir integração com *Radius* para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída para internet, para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

Suporte a autenticação Kerberos.

Solução Principal – Solução de Gerenciamento e Monitoramento

A solução de gerência deverá ser separada dos gateways de segurança.

A gerência deve permitir centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento.

Deve estar licenciada para gerenciamento de, pelo menos, quatro (4) *Appliances* (internos e externos) de segurança, além dos *softwares* envolvidos.

Caso a solução possua licenças relacionadas a armazenamento, deve ser fornecida, no mínimo, a de capacidade diária de 150 GB de armazenamento de log indexados, assim como deve suportar uma capacidade mínima de 10 TB de armazenamento total de logs indexados.

O gerenciamento da solução deve suportar acesso via SSH, além de software cliente ou interface WEB (HTTPS).

A solução de gerência deve oferecer possibilidade de acesso sem necessidade da Java.

Em caso de software, o mesmo deve suportar implementação em hardware de outra fabricante, sendo preferencialmente executado em ambiente virtualizado VMWARE, para que a funcionalidade de gerenciamento não seja comprometida quando o *appliance* estiver operando em qualquer um de seus limites de capacidade. Caso haja a necessidade de o software rodar de modo *baremetal* ou em outra solução *hipervisor*, a CONTRATADA deverá prover o equipamento.

Caso haja necessidade de instalação de cliente para administração da solução, este deve ser compatível com sistemas operacionais Windows 10 ou superior ou Linux (Fedora, Ubuntu e Red Hat Enterprise Linux) em suas últimas versões.

Deve manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios.

O gerenciamento deve permitir/possuir:

- Criação e administração das políticas da solução;
- Monitoração de logs em tempo real;
- Ferramentas de investigação de logs;
- Debugging, sendo que este pode ocorrer no próprio appliance;
- Captura de pacotes, sendo que esta pode ocorrer no próprio appliance;
- Acesso concorrente de administradores, pelo menos para leitura;
- Deve permitir análise em tempo real da navegação do usuário, identificando-o por login, IP ou MAC;
- Deve permitir usar palavras chaves para facilitar identificação de regras;
- Deve permitir monitorar, via SNMP, falhas de hardware, como fontes, discos, utilização ao licenciamento total suportado/licenciado e número de sessões estabelecidas.

- Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- Autenticação integrada ao Microsoft Active Directory, base de dados local ou Radius;
- Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
- Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QoS e demais regras;
- Criação de regras que fiquem ativas em horário definido;
- Criação de regras com data de expiração;
- Backup das configurações e rollback de configuração para a última configuração salva;
- Suportar rollback de Sistema Operacional para a última versão local;
- Habilidade de upgrade via SCP, TFTP ou interface de gerenciamento;
- Validação de regras antes da aplicação;
- Validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing);
- Deve possibilitar a visualização e comparação de configuração atual, configuração anterior e configurações antigas;
- Deve possibilitar a integração com soluções de SIEM de mercado;
- Deve ter a capacidade de manter logs indexados por um período mínimo de 30 (trinta) dias;
- Permitir pesquisa nos logs através de informações do endereço de origem e/ou destino, porta de origem e/ou destino, serviço utilizado, funcionalidade do firewall, ações envolvidas, usuário logado e aplicação utilizada, dentre outros;
- Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
- Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

- Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spyware), URLs e filtro de arquivos (quando aplicável), para melhor diagnóstico e resposta a incidentes;
- O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
- Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spyware), entre outros
- Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spyware), bem como de URLs ou categorias de URLs que passaram pela solução.
- Deve possuir mecanismo “drill-down” para navegação nos logs/relatórios em RealTime;
- Nas opções de “drill-down”, ser possível identificar o usuário que fez determinado acesso;
- Deve ser possível exportar os logs em CSV ou XML;
- Deverá ser possível aplicar configurações aos appliances de firewall durante momentos de tráfego alto, bem como em momentos de alta utilização de CPU e memória;
- Deve permitir configurar a rotação dos logs.
- Exibição de, pelo menos, as seguintes informações, de forma histórica e em tempo real, atualizado de forma automática:
  - Situação do dispositivo e do cluster;
  - Principais aplicações;
  - Administradores autenticados na gerência da plataforma de segurança;
  - Número de sessões simultâneas;
  - Status das interfaces;
  - Consumo de recursos do appliance.
- Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

- Resumo gráfico de aplicações utilizadas;
- Principais aplicações por utilização de largura de banda de entrada e saída;
- Principais aplicações por taxa de transferência de bytes;
- Principais hosts por número de ameaças identificadas;
- Atividades de um usuário específico e grupos de usuários, incluindo aplicações acessadas, categorias de URL, e ameaças (IPS, Antivírus e Anti-Spyware) vinculadas a este tráfego.

- Deve permitir a criação de relatórios personalizados.
- Possibilidade de exportar, copiar ou salvar relatórios e gráficos gerados.
- Gerar alertas automáticos via: E-mail, SNMP e Syslog.

Solução Principal – Firewall de Contingência

Cada *appliance* deve suportar, no mínimo, 1 (um) Gbps de *throughput* com as seguintes funcionalidades habilitadas simultaneamente:

- Firewall, controle de aplicação, IPS, antimalware/antivirus e VPN client-to-site.
- VPN client-to-site deve suportar, pelo menos, 20 usuários simultâneos.
- Cada appliance deve suportar, no mínimo, 1 (cinquenta) Gbps de throughput de firewall com identificação de aplicação;
- Cada appliance de firewall de contingência deve suportar, no mínimo, 1 Gbps de throughput para VPN.
- Cada appliance de firewall de contingência deve suportar, no mínimo, 1 Gbps de throughput para Threat Prevention com Firewall, antivírus/antimalware, URL/DNS Security, IPS, controle de aplicação, recursos ativo-passivo e logging ativos.

As configurações (i.e políticas, QoS, ACL, IPS/IDS, antimalware etc.) serão os mesmos aplicados aos firewalls internos/externos, de acordo com os recursos habilitados simultaneamente no firewall de contingência.

Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 110 e 240 VAC que permitam hot-swap. Preferencialmente, utilizar padrão de conexão C13/C14.

Cada firewall deverá ter, pelo menos, 4 interfaces de 1Gbps do tipo Ethernet ou SFP.

Possuir, pelo menos, 1 interface UTP 1 GB dedicada para gerência.

Todas as interfaces solicitadas nos *appliances* para atendimento dos requisitos devem estar licenciadas e habilitadas para uso imediato, incluindo seus *transceivers*.

Licenciamento de interfaces

Todas as interfaces elétricas RJ45, óticas SFP+ e óticas SFP28 solicitadas nos equipamentos devem estar licenciadas de maneira permanente, ou seja, sem data de expiração, sendo habilitadas após a emissão do termo de recebimento definitivo de ativação, incluindo seus transceivers. Caso durante o processo de implantação haja necessidade de licenças provisórias, a CONTRATADA deve fornecer para a CONTRATANTE sem custo adicional para que o prazo de 60 meses não seja afetado. Se não for possível o uso de licenças provisórias com características idênticas as licenças definitivas, a CONTRATADA deverá estender o prazo das licenças sem custo para a CONTRATANTE durante a fase de implantação.

O licenciamento permanente junto com a solução deverá prover todos os recursos que são exigidos pela CONTRATANTE os quais inclui:

- Recursos de Firewall;
- VPN na modalidade site-to-site (IPSEC VPN);
- Suportar SSL VPN tipo remote-acess para, no mínimo, 1000 usuários concorrentes nos firewalls externos e internos e 500 usuários no firewall de contingência;
- Recurso de inspeção SSL;
- Modo Cluster Ativo-Passivo;

As funcionalidades adicionais não descritas nesse documento, porém vinculadas ao licenciamento acima devem estar ativas para uso.

As funcionalidades que dependem de subscrição como proteção contra malware, Identificação de Usuário e detecção e prevenção de invasões (IDS e IPS) deverão ter validade de período igual à Garantia Estendida presente nesse documento (60 meses).

Deve ser incluído qualquer licenciamento necessário para atendimento dos requisitos de arquitetura tecnológica que não foram destacados nos itens anteriores.

Serviço de operação e sustentação

Serviços de operação e sustentação de solução de firewall (equipamentos e gerenciador da solução) prestado por 1 (um) profissional técnico da CONTRATADA ou do Fabricante na CONTRATANTE.

Caberá a CONTRATADA a prestação dos serviços de operação e sustentação dos equipamentos da solução de 60 (sessenta) meses, a contar do término da Operação Assistida (EVENTO 6).

O profissional responsável por prover o serviço de operação e sustentação do ambiente deverá ter certificação do FABRICANTE em relação aos produtos fornecidos pela CONTRATADA ou ser funcionário vinculado ao FABRICANTE da solução.

A exigência de capacidade técnica acima e experiência prévia tem por objetivo comprovar experiência anterior na realização de serviços similares, proporcionais à dimensão e complexidade do objeto a ser executado, visando assegurar que a Administração contratará empresas e profissionais que possam incumbir-se adequadamente do objeto contratado. Os equipamentos envolvidos na especificação desta contratação tratam de tecnologias (protocolos) complexos, como VPN IPSec, SSL VPN, Threat Detection, análise de vulnerabilidades em arquivos e dados. Estes equipamentos, se mal configurados, podem indisponibilizar a comunicação segura

entre a JF3R e o mundo externo, incluindo, mas não se limitando, a tráfego com usuários em teletrabalho, outras entidades públicas e privadas, usuários externos que acessam informações em sistemas processuais e usuários internos que necessitam acessar serviços externos. Também destacamos que a má configuração dos equipamentos pode, ainda, expor a rede de dados da JF3R a ataques externos que visam extrair dados ou gerar indisponibilidade dos serviços da instituição. Os conhecimentos técnicos necessários para implementar as tecnologias acima não são triviais e exigem conhecimento prévio e comprovado das tecnologias do produto.

O profissional deverá estar disponível exclusivamente para a CONTRATANTE pelo período de 64 horas mensais, sendo 2 dias por semana. Excepcionalmente, em comum acordo entre as partes, a frequência semanal e/ou diária poderá ser alterada, porém o total de horas mensais não poderá ser maior que 64 horas.

A critério da CONTRATANTE a modalidade de trabalho poderá ser presencial, híbrida ou remota.

Os serviços de operação e sustentação são distintos dos serviços de garantia e de assistência técnica dos equipamentos a serem fornecidos, os quais estão descritos nos Requisitos de Garantia e Requisitos de Arquitetura Tecnológica.

Os serviços de operação e sustentação abrangem atividades que não são cobertas pela garantia ou pelo suporte técnico do fabricante, visto que esses visam garantir a resolução de problemas referentes a falhas e defeitos nos equipamentos ofertados, enquanto aqueles visam fundamentalmente viabilizar a administração e a operação de tais equipamentos.

Os serviços de operação e sustentação não abrangem as atividades referentes à primeira instalação e configuração inicial dos equipamentos ofertados.

Em sua essência, tais serviços visam auxiliar a equipe técnica do contratante na administração e na operação dos equipamentos ofertados, no âmbito das atividades que exijam conhecimentos com maior grau de complexidade e que possam impactar negativamente no negócio caso sejam executadas com insucesso.

Os serviços de operação e sustentação dos equipamentos da solução ofertados deverão contemplar a execução das atividades enumeradas abaixo:

- Subsidiar a CONTRATANTE na elaboração de projetos de estruturas físicas e lógicas de dos firewalls;
- Gerar relatórios e gráficos a respeito de incidentes ou problemas de segurança;
- Detectar, de modo proativo, possíveis problemas de segurança relacionado a solução;
- Manter organização de políticas e regras aplicadas, de acordo com orientação e padrões da CONTRATANTE;
- Analisar eventos, atender solicitações, resolver incidentes e problemas, realizar mudanças e analisar e resolver eventos em serviços e ativos relacionados;
- Instalar, migrar e customizar softwares aplicativos e equipamentos relacionados ao firewall;
- Definir e apoiar na definição de requisitos de monitoramento e garantir que todas as necessidades de monitoramento e geração de eventos para a correta interpretação dos eventos;
- Diagnosticar gargalos e problemas de tráfego do firewall;
- Analisar periodicamente a solução para validar a necessidade de updates;
- Instalar atualizações da solução e dos recursos agregados;
- Configurar ACLs;
- Configurar rotas estáticas e/ou dinâmicas;
- Configurar regras de IPS;
- Configurar regras de NAT;
- Emitir relatórios de hosts/usuários com maiores incidentes;

- Emitir relatórios de incidentes;
- Troubleshooting relacionado a eventos, incidentes e solicitações na solução;
- Gerenciar a solução em conjunto com a equipe técnica judiciária;
- Apoiar na elaboração de plano de melhoria do firewall;
- Configurar e validar backup da solução;
- Apoiar a equipe técnica na elaboração de Requisições de Mudanças para alterações no ambiente da solução de firewall.

- **Requisitos de Projeto e de Implementação:**

Após a assinatura do Contrato, a Contratada deverá marcar uma reunião inicial (Requisito Temporal – Evento 2) com a equipe técnica da CONTATANTE de planejamento do projeto para *kickoff*, alinhamentos, levantamento de informações e quaisquer outras informações necessárias para elaboração de documentação inicial.

A CONTRATADA deverá realizar uma avaliação preliminar do ambiente de TI da CONTRATANTE, incluindo uma análise da infraestrutura atual, para identificar quaisquer prerrequisitos ou necessidades de adaptação antes da implementação.

Deverá ser entregue Plano de Projeto (Requisito Temporal – Evento 3) contendo, pelo menos, os seguintes artefatos: Termo de Abertura de Projeto, Declaração de Escopo, Matriz RACI, Cronograma com *milestones*, Estrutura Analítica do Projeto, Análise de Riscos e Recursos Humanos. Adicionalmente, deverá conter aspectos técnicos da implantação como detalhes de migração, procedimentos e testes a serem realizados.

Poderão ser utilizadas as seguintes metodologias/guias para gerenciamento e acompanhamento de projeto: PMBoK 6ª edição ou 7ª edição. .

As soluções fornecidas devem ser totalmente compatíveis com a infraestrutura de TI existente da CONTRATANTE, devendo funcionar sem nenhum tipo de alerta.

A CONTRATADA é responsável pela instalação completa e configuração dos equipamentos e software, garantindo que estes estejam operacionais e otimizados para o ambiente da CONTRATANTE.

A CONTRATADA deverá manter um canal de comunicação aberto e contínuo com a CONTRATANTE, fornecendo relatórios regulares sobre o progresso da implementação, incluindo qualquer desafio ou desvio do plano original.

Toda reunião deverá gerar uma ATA que será assinada pela CONTRATADA e CONTRATANTE.

As documentações geradas durante o projeto deverão ser entregues após o período de operação assistida (Requisito Temporal – Evento 6).

Como exemplo, destacam-se as documentações técnicas referentes a configurações aplicadas, desenhos de arquitetura, identificação de interfaces/portas nos switches, políticas criadas e aplicadas (segurança, acesso, QoS etc.).

Junto as documentações técnicas, a CONTRATADA deverá estabelecer um plano de recuperação de desastres com procedimentos claros para restaurar rapidamente os serviços em caso de falhas críticas ou eventos inesperados.

A solução será recebida pela CONTRATANTE conforme abaixo:

TERMO	SITUAÇÃO DE EMISSÃO
Recebimento Provisório dos equipamentos	Em até 10 dias corridos ,após Entrega dos equipamentos (EVENTO 4) e a conferência física pela equipe da CONTRATANTE, não sendo vinculante a instalação.
Recebimento Definitivo dos equipamentos	Em até 10 dias corridos ,após emissão do Termo de Recebimento Provisórios dos equipamentos (EVENTO 5) e validação dos equipamentos adquiridos e a nota fiscal emitida
Recebimento Provisório da ativação de licenças	Em até 10 dias corridos , após verificação da ativação de licenças (EVENTO 8) via sistema ou portal do FABRICANTE pela equipe

	da CONTRATANTE
Recebimento Definitivo da ativação de licenças	Em até 10 dias corridos , aós emissão do Termo de Recebimento Provisório da ativação de licenças (EVENTO 11) e verificação do funcionamento das licenças nos equipamentos adquiridos.
Recebimento Provisório dos serviços de implantação	Em até 10 dias corridos , após instalação física da solução, configuração e integração, testes e operação assistida (EVENTO 7)
Recebimento Definitivo dos serviços de serviços de implantação	Em até 10 dias corridos , após entrega da documentação de implantação (EVENTO 12)
Recebimento Provisório dos serviços de treinamento	Em até 10 dias corridos , após término do treinamento (EVENTO 9)
Recebimento Definitivo dos serviços de treinamento	Em até 10 dias corridos , após emissão do Termo de Recebimento Provisório dos serviços de treinamento (EVENTO 13) e emissão dos certificados de conclusão
Recebimento Provisório dos serviços de operação e sustentação	Mensalmente, após validação dos níveis de serviços pela CONTRATADA, em até 10 dias corridos
Recebimento definitivo dos serviços de operação e sustentação	Em até 10 dias corridos , após o fim do período de 60 (sessenta) meses
Recebimento Definitivo dos serviços de suporte técnico, atualizações e garantia	Em até 10 dias corridos , após o fim do período de 60 (sessenta) meses

- **Requisitos de Implantação:**

A implantação não deve interromper as operações diárias da CONTRATANTE e deve ser feita de forma a minimizar qualquer possível tempo de inatividade.

Todas as atividades realizadas deverão seguir as boas práticas sugeridas pelo fabricante da ferramenta, não sendo aceitas ações que não tenha respaldo documental.

A CONTRATADA é responsável por quaisquer materiais para a implantação de serviço, por exemplo: Cabo par trançado, fibra óptica, transceivers, cabos de energia, adaptadores elétricos, velcro, cabo de crimpagem etc.

A implantação envolverá as seguintes atividades:

- Instalação física e lógica:

- Deverá ser disponibilizado, em racks localizados nos data centers da CONTRATANTE, espaço físico para os novos equipamentos, preferencialmente em racks distintos com PDU's independentes para cada PSU (Fonte de Energia). A fixação ocorrerá através de conjunto a ser fornecido junto com o equipamento.

- Deverá ser disponibilizado em ambiente virtual VMware da CONTRATANTE uma solução de gerenciamento centralizado. Caso a solução seja um appliance físico, deverá ser instalado em rack disponibilizado nos data centers da CONTRATANTE.

- Ao final, a CONTRATADA deverá providenciar relatório fotográfico da instalação física para envio à CONTRATANTE assim que a tarefa for concluída.

- Configuração:

- Refere-se à configuração lógica do equipamento. Nesta etapa, as políticas, regras e quaisquer configurações do equipamento legado deverá ser migrada para o novo equipamento, além de criação de novas regras e políticas que se mostrarem necessárias. Caso haja necessidade de rede para configuração, preferencialmente, o processo deverá ocorrer em ambiente apartado do ambiente produtivo, em uma rede virtual (VLAN) distinta do ambiente produtivo para que não haja influência na operação.

- A CONTRATADA deve validar os dados criados nos novos equipamentos comparando-os com os dados dos equipamentos legados, garantindo a integridade das configurações.

- Os equipamentos devem ser configurados em sua última versão estável com seus patches (releases) mais recentes instalados. Não serão aceitas funcionalidades que estejam executando em builds não-estáveis (alpha, beta etc.) ou modificações personalizadas diretamente em código.

- Ao final, a CONTRATADA deverá formalizar, por email, a conclusão da configuração dos equipamentos da solução, indicando com prints de tela o que foi configurado, tão logo essa tarefa seja concluída.

- Integração:

- Deverão ser conectados todos os cabos para o funcionamento pleno da ferramenta. Destaca-se que na etapa de configuração, somente os cabos necessários para configuração serão conectados.

- A CONTRATADA ficará responsável pela organização e identificação (etiquetagem) de todos os cabos (rede, óticos e/ou elétricos) que serão utilizados e instalados na infraestrutura da CONTRATANTE.

- A integração deve ser efetuada de maneira a não interromper as operações existentes, garantindo uma transição suave e sem interrupções para os novos sistemas e serviços. A abordagem de como será feita deverá ser descrita no Plano de projeto.

- Testes:

- Os testes têm por objetivo validar que todos os requisitos solicitados e apresentadas na proposta da CONTRATADA estão sendo atendidos.

- Os testes serão, preferencialmente, realizados em ambiente lógico apartado da rede produtiva da CONTRATANTE.

- Deverão ser realizados, pelo menos, os seguintes tipos de testes: penetração (pen test), desempenho, segurança funcional, resiliência, escalabilidade.

- Como testes de penetração entende-se a simulação de ataques reais contra o NGFW para identificar e explorar vulnerabilidades. Como exemplos, testes de bypass de Firewall (tráfego camuflado, túneis e/ou encapsulamento), exploração de vulnerabilidades conhecidas, injeção de pacotes maliciosos, análise de tráfego criptografado (esconder atividades maliciosas dentro de tráfego criptografado) etc.

- Como testes de desempenho entende-se avaliar a capacidade do NGFW lidar com as cargas (workloads) exigidos nos requisitos. Como exemplos, validar os requisitos de throughput e conexões simultâneas solicitadas nesse Termo de Referência/Edital, verificar a latência de resposta RTT (Round-Trip Time) entre o NGFW e um servidor virtual localizado na rede interna, verificar o máximo de carga que os equipamentos suportam em relação a thoughtput e conexões simultâneas

(sobrecarga de conexões) dentro das limitações da rede interna, inspeção profunda de pacotes (Deep Package Inspection) com a capacidade do NGFW analisar análises detalhadas de pacotes (relacionado aos testes de penetração), validar quantidade de conexões na VPN IPSEC e SSL etc.

- Como testes de segurança funcional entende-se verificar as funcionalidades solicitadas pela CONTRANTE como firewall, IPS/IDS, controle de aplicações, QoS, antivírus ou malware, descriptografia e inspeção de tráfego SSL/TLS, filtro de conteúdo, VPN IPSEC/SSL. Como exemplos, verificar intrusões (validado durante o pen test), validar se sites proibidos (adultos, apostas, pirataria etc.) são bloqueados, validar bloqueio de tráfego através de inspeção SSL/TLS (validado durante o pen test), verificar prevenção de ameaças avançadas através de evasão de assinatura em que um malware conhecido sofra metamorfose e o NGFW é capaz de identificar esse comportamento e bloquear, validar as políticas criadas e migradas alterando a ordem e percebendo o comportamento da ferramenta, validar se as regras de QoS estão sendo aplicadas corretamente comparando o comportamento da ferramenta quando estas são desativadas etc.

- Para os testes de segurança funcional, os testes unitários a seguir deverão ser obrigatoriamente serem executados:

I. Teste de funcionalidades de gerência centralizada e apartada:

O objetivo é mostrar que o appliance de segurança e a gerência centralizada são capazes de operar de maneira apartada um do outro dentro da solução;

a. O appliance de segurança (NGFW) deve ser desligado e a gerência centralizada mantida ligada.

b. Deve ser configurada na gerência uma política que bloqueia o acesso do cliente da Rede Interna ao site do Facebook;

c. O appliance de segurança deve ser religado e a nova política aplicada;

d. A gerência centralizada deve ser desligada;

e. Deve ser feito o acesso ao Facebook a partir do cliente (espera-se que seja bloqueado) e um acesso a outro site qualquer (espera-se que seja permitido);

f. A gerência centralizada deve ser religada;

g. Deve ser exibido na console de gerência os logs do acesso que foi bloqueado e do que foi permitido;

II. Teste de funcionalidades de acesso entre redes:

O objetivo é verificar se o Firewall consegue liberar determinados protocolos a uma rede específica.

a. Deve ser feito dois tipos de acesso a partir da rede interna para rede Servidores e para rede DMZ.

b. Acesso 1: utilizando protocolo https e sendo liberado o acesso;

c. Acesso 2: utilizando protocolo ssh e sendo bloqueado para a DMZ e liberado para a rede servidores;

d. Deverá ser feito um tipo de acesso externo com origem em um cliente vpn com destino a rede servidores.

III. Teste de funcionalidades de auditoria:

O objetivo é mostrar que a solução é capaz de mostrar as informações detalhadas de auditoria sobre as mudanças realizadas.

a. Deverá ser exibido na console de gerência os registros que demonstrem:

b. O horário da aplicação das últimas políticas;

c. A mudança realizada para bloqueio do Facebook;

d. O horário da mudança;

e. O administrador que realizou a mudança.

IV. Teste de disponibilidade

O objetivo é mostrar que o nó passivo do cluster assumirá a operação quando o nó ativo ficar indisponível.

b. Deve ser desligada a PDU do nó ativo.

c. Verificar se o nó passivo assumiu as operações com RTO=0.

d. Ligar o appliance do nó ativo.

e. O nó ativo deverá assumir o controle das operações.

V. Teste de funcionalidades de desempenho do IPS:

O objetivo é verificar o comportamento na ferramenta com a funcionalidade IPS ativa e se atinge os requisitos mínimos de troughput solicitados.

a. A LICITANTE CONVOCADA deverá utilizar alguma solução de geração de tráfego com o intuito de gerar diversos tipos de ataque contra a solução a fim de validar que as assinaturas estão habilitadas e realizando devidamente os bloqueios.

b. Os ataques a serem simulados serão feitos como se estivessem conectados vindos da internet.

c. A partir da gerência do appliance deva ser possível verificar os logs das tentativas de acesso malsucedidas.

d. A LICITANTE CONVOCADA deverá também demonstrar quais assinaturas foram utilizadas durante a sessão de teste.

e. A LICITANTE CONVOCADA deverá realizar testes de simulação com ataques diversos com o intuito de validar, minimamente, que o IPS/IDS funciona a contento com diversas assinaturas ativadas e diversos ataques realizados simultaneamente.

VI. Teste de disponibilidade

O objetivo é mostrar que o nó passivo do cluster assumirá a operação quando o nó ativo ficar indisponível.

b. Deve ser desligada a PDU do nó ativo.

c. Verificar se o nó passivo assumiu as operações com RTO=0.

d. Ligar o appliance do nó ativo.

e. O nó ativo deverá assumir o controle das operações.

- Como testes de resiliência entende-se verificar a capacidade do NGFW de se recuperar de falhas e/ou ataques e continuar a proteger a rede de forma eficaz. Como exemplos, validar o comportamento ativo-passivo da solução desligando a ferramenta ativa e verificando se a ferramenta passiva assume sem interrupções na proteção de rede (RTO=0), validar desastres ambientes desligando as fontes de energia com o equipamento em operação e verificando se a inicialização ocorre sem problemas após a normalização, validar se as políticas e regras estão persistentes após uma falha ou reinicialização da ferramenta, validar o processo de atualização de firmware e aplicação de patches, validar a conectividade dos equipamentos simulando problemas pontuais nas interfaces de redes, validar a restauração de backup etc.
- Como testes de escalabilidade entende-se verificar a capacidade do NGFW lidar com diferentes cargas de trabalho (workloads). Como exemplos, aumentar gradualmente a carga (conexões simultâneas e throughput) recebida pelo equipamento e validar se o aumento da utilização de recursos condiz com o aumento de carga, aumentar em grande número a quantidade de políticas e regras no firewall e verificar se o desempenho da ferramenta é comprometido etc.
- Além dos testes descritos, todos os testes recomendados pelo fabricante devem ser realizados.
- Preferencialmente, o seguinte modelo deverá ser adotado para os testes:

CENÁRIO DE TESTE	CONDIÇÃO DE ENTRADA	CONDIÇÃO DE SAÍDA	RESULTADO ESPERADO	STATUS

- Operação Assistida:

- É o período em que uma mão de obra da Contratada ficará alocada nas dependências da CONTRATANTE, monitorando as atividades dos equipamentos adquiridos pelo período de 30 dias corridos. Caso seja necessário, deverão ser aplicadas configurações de tunning para melhoria de desempenho e/ou disponibilidade.

- Os acionamentos da CONTRATADA pela CONTRATANTE, durante o período de operação assistida, deverão ser tratados com o nível de serviço definidos para prioridade alta da tabela de Nível Mínimo de Serviço.

- A operação assistida durará iniciará após a finalização do processo de testes.

- A critério da CONTRATANTE, a operação assistida poderá ser na modalidade presencial, híbrida ou remota.

- Encerramento:

- A CONTRATADA deverá comprovar o registro no portal da FABRICANTE dos partnumbers, ou similar, que compõem a solução, se aplicável.

- É o período em que o projeto se encerra com a emissão do Termo de Recebimento Definitivo de Implantação.

- **Requisitos de Garantia:**

- Garantia Contratual dos Serviços: O prazo de garantia contratual dos serviços (suporte técnico), complementar à garantia legal, será de no mínimo 60 (sessenta) meses, contado a partir de a assinatura do **termo de recebimento definitivo da ativação de licenças**. Esta garantia é exigida para assegurar a prestação continuada de serviços com a qualidade esperada e a correção de possíveis defeitos ou falhas que possam surgir durante o período estabelecido. Ressalta-se que durante a fase de implantação (instalação, configuração, integração, testes e operação assistida), caso haja necessidade de licenças válidas, deverão ser fornecidas licenças provisórias por parte da CONTRATADA para a CONTRATANTE,

não sendo considerados os 60 meses. Essas licenças provisórias deverão ter as mesmas características das licenças definitivas adquiridas pela CONTRATANTE. Caso não haja a possibilidade, as licenças deverão ter seu período estendido durante a fase de implantação para que não seja afetado o período de 60 meses.

- Garantia Contratual dos Bens: Considerando que os serviços envolvem o fornecimento de equipamentos de alta criticidade para a segurança da informação e infraestrutura de rede da CONTRATANTE, a garantia contratual dos bens (hardware) será de, no mínimo, 60 (sessenta) meses, contados a partir da emissão do **termo de recebimento definitivo da ativação de licenças**. Este período visa cobrir quaisquer defeitos de fabricação, funcionamento inadequado ou outras falhas que possam comprometer a integridade do sistema e a continuidade dos serviços públicos prestados pela instituição. Ressalta-se que durante a fase de implantação (instalação, configuração, integração, testes e operação assistida), os equipamentos deverão possuir garantia legal e/ou garantia provisória, não sendo considerados dentro dos 60 meses.

- A Contratada deverá prover para a CONTRATANTE um usuário cadastrado em portal do fabricante, para download de firmware, patches e consulta documentos técnicos durante o período de garantia.

- Caso a garantia provida seja do Fabricante, a CONTRATADA deverá prover para CONTRATANTE um usuário para utilização de portal de suporte técnico.

- Serão aceitos modelo de suporte híbrido, em que os primeiros níveis são atendidos pela CONTRATADA e os últimos níveis pelo Fabricante do equipamento.

- Encargos da Garantia: Todos os custos e encargos relacionados à execução dos serviços de garantia contratual e assistência técnica necessários durante o prazo de garantia dos serviços e dos bens serão de responsabilidade integral da CONTRATADA, sem oneração adicional para a CONTRATANTE.

- **Requisitos de Experiência Profissional:**

Os serviços de assistência técnica e garantia deverão ser prestados por técnicos da CONTRATADA ou da FABRICANTE. .

A licitante provisoriamente vencedora do certame deverá apresentar declaração formal de que irá disponibilizar profissional responsável pelo serviço de operação e sustentação, respeitando as especificações em que esse serviço está definido.

A CONTRATANTE poderá requerer, antes da execução dos serviços, a comprovação da capacitação dos profissionais através de apresentação de documentação ou certificados emitidos pela fabricante da solução. A comprovação poderá ser feita por meio de certificados de participação em treinamento ou carta emitida pela fabricante do produto.

O profissional responsável por prover o serviço agregado de operação e sustentação do ambiente deverá ter certificação do fabricante em relação aos produtos fornecidos pela CONTRATADA ou ser funcionário vinculado ao fabricante do Produto. Caso não haja certificação para as ferramentas, serão aceitos certificados de conclusão de treinamento com atestado(s) que comprovem as atividades de operação relacionadas às ferramentas adquiridas.

A exigência de capacidade técnica acima e experiência prévia tem por objetivo comprovar experiência anterior na realização de serviços similares, proporcionais à dimensão e complexidade do objeto a ser executado, visando assegurar que a Administração contratará empresas e profissionais que possam incumbir-se adequadamente do objeto contratado. Os equipamentos envolvidos na especificação desta contratação tratam de tecnologias (protocolos) complexos, como VPN IPSec, SSL VPN, Threat Detection, análise de vulnerabilidades em arquivos e dados. Estes equipamentos, se mal configurados, podem indisponibilizar a comunicação segura entre a JF3R e o mundo externo, incluindo, mas não se limitando, a tráfego com usuários em teletrabalho, outras entidades públicas e privadas, usuários externos que acessam informações em sistemas processuais e usuários internos que necessitam

acessar serviços externos. Também destacamos que a má configuração dos equipamentos pode, ainda, expor a rede de dados da JF3R a ataques externos que visam extrair dados ou gerar indisponibilidade dos serviços da instituição. Os conhecimentos técnicos necessários para implementar as tecnologias acima não são triviais e exigem conhecimento prévio e comprovado das tecnologias do produto.

- **Formação da Equipe:**

Para a implantação da solução, a Contratada deverá prover, no mínimo, dois perfis de profissionais:

- Gerente de projeto: responsável por gerenciar a implantação, emitindo toda documentação solicitada com base nos requisitos de projeto. Será necessária comprovação de atuação como Gerente de Projeto através de atestado(s)–no momento da assinatura do contrato.

- Técnico Especialista: responsável pela implantação da Solução. Deverá comprovar atuação em instalação e configuração de NGFW com características similares (nível de hardware e funcionalidades) com os produtos adquiridos. A comprovação dar-se-á através de certificação emitida pelo fabricante ou currículo profissional que comprovem as atividades de implantação relacionadas às ferramentas adquiridas, no momento da assinatura do contrato.

- **Requisitos de Metodologia de Trabalho:**

O fornecimento dos equipamentos está condicionado ao prazo de 60 (sessenta) dias após a assinatura do contrato.

O andamento do fornecimento dos equipamentos dever ser acompanhado pela CONTRATADA, que dará ciência de eventuais acontecimentos ao contratante.

A entrega dos equipamentos e periféricos deverão ser em endereços a serem definidos pela CONTRATANTE no Contrato.

Estes requisitos definem a forma de demanda, os instrumentos e mecanismos necessários para o fornecimento dos equipamentos, bem como a definição da rotina de execução e operação e meios de comunicação entre as partes.

Todas as demandas devem ser formalizadas por meio de solicitações escritas, enviadas via e-mail ou através do portal online personalizado.

As solicitações devem incluir todas as informações necessárias para a completa compreensão e execução das tarefas, incluindo, mas não se limitando a, especificações técnicas, prazos e prioridades.

A CONTRATADA deve fornecer documentação completa e detalhada sobre a configuração dos sistemas, procedimentos de operação e manutenção, e qualquer outra informação técnica relevante. Essa documentação poderá ser enviada em formato digital, em até 5 dias úteis a partir do término do atendimento.A CONTRATADA deve utilizar um portal online personalizado para o gerenciamento das demandas, controle de chamados, acompanhamento de status e disponibilização de relatórios.

Deve ser fornecido acesso ao portal para a equipe da CONTRATANTE.

A CONTRATADA deve manter um registro detalhado de todas as atividades realizadas, incluindo a data e hora de cada ação, pessoa responsável e descrição do trabalho executado.

Os equipamentos deverão possuir monitoramento ativo e contínuo. Qualquer incidente no ambiente deverá gerar um e-mail para a CONTRATADA de forma automatizada. Esse e-mail gerará a abertura de um chamado técnico.

A CONTRATADA deverá fornecer relatório de atendimento técnico, referente a cada chamado, contendo no mínimo as seguintes informações:

- Data e hora da abertura do chamado;
- Data e hora do início do atendimento;
- Responsável pelo atendimento da solicitação;

- Motivo da ocorrência (indicação do defeito);
- Nível de criticidade da ocorrência;
- Status do chamado (aberto, em tratamento, fechado etc.);
- Data e hora do fechamento do chamado;
- Contato da CONTRATANTE que autorizou o encerramento do chamado;
- Solução adotada (resolução).

O portal online da CONTRATADA deverá conter, pelo menos, as seguintes informações:

- Permitir acesso mediante informação de credenciais de acesso (usuário e senha)
- Nível de severidade de acordo com o Nível de serviço.
- Quantidade de incidentes e relação dos serviços.
- Chamados técnicos registrados.
- E-mail automático de atendimento técnico com as seguintes informações:
- Data e hora da abertura do chamado.
- Data e hora do início do atendimento.
- Responsável pelo atendimento da solicitação.
- Motivo da ocorrência (indicação do defeito).
- Status do chamado (aberto, em tratamento, fechado etc.).
- Data e hora do fechamento do chamado.
- Solução adotada (resolução).
- Possibilidade que todos da equipe técnica da CONTRATANTE visualizem todos os chamados, independente de quem é o solicitante.

A CONTRATADA deverá criar uma base de dados com os históricos de chamados realizados pela CONTRATANTE que deverá ser consultada sempre que o profissional técnico responsável pelo atendimento for iniciar um atendimento. A CONTRATANTE poderá a qualquer momento solicitar relatórios referentes a esta base de dados contendo os históricos dos seus chamados.

Toda manutenção preventiva ou atualizações de software deverá passar por Requisição de Mudança da Contratante.

A Contratada deverá emitir toda documentação necessária para essas atividades para aprovação em reunião de Gestão de Mudança.

A CONTRATADA deve fornecer um plano de contingência para garantir a continuidade dos serviços em caso de falhas ou interrupções. Os serviços deverão ser executados sem impacto na utilização do ambiente de TI da CONTRATANTE, de forma que os subsistemas mais críticos deverão ser executados em horário noturno e/ou finais de semana, a critério da CONTRATANTE.

Os meios de comunicação primários entre a CONTRATADA e a CONTRATANTE serão o e-mail, telefone e o portal online personalizado.

A CONTRATADA deve disponibilizar um canal de atendimento 24x7 para emergências, com capacidade de resposta imediata.

Deve-se manter um registro de todas as comunicações entre as partes, incluindo e-mails, registros de chamadas e atas de reuniões, que serão armazenados de forma segura e acessíveis para consulta quando necessário.

Deve haver uma programação regular de reuniões de acompanhamento, preferencialmente mensais, para revisão do progresso das atividades e planejamento de futuras ações.

Relatórios periódicos devem ser gerados e fornecidos à CONTRATANTE, incluindo análises de desempenho, incidentes resolvidos, pendências e recomendações de melhorias. A CONTRATANTE definirá e ajustará a periodicidade

desses relatórios durante a vigência do contrato, buscando a periodicidade mais adequada de acordo com a experiência da solução.

A CONTRATADA deve assegurar a rastreabilidade de todas as atividades realizadas, fornecendo evidências documentais para cada ação executada.

A CONTRATADA deve manter um registro de todas as mudanças realizadas, incluindo justificativas, procedimentos adotados e impactos observados.

Qualquer alteração nos serviços, equipamentos ou metodologia de trabalho deve ser comunicada à CONTRATANTE com antecedência. Isso inclui alterações nos canais de atendimento, como endereço do portal de atendimento, credenciais de acesso, telefones e e-mails de contato da CONTRATADA.

Todas as atividades devem ser conduzidas em conformidade com as normas de segurança da informação e políticas internas da CONTRATANTE.

Suporte técnico especializado deve estar disponível para resolver dúvidas e problemas relacionados à utilização dos equipamentos e serviços.

A CONTRATADA deverá disponibilizar lista de equipamentos com alertas de informações noticiadas pelo fabricante dos equipamentos contratados, data de fim de suporte conforme anunciado pelo fabricante por equipamento.

A CONTRATADA deve garantir a proteção de dados e informações confidenciais, adotando medidas de segurança adequadas para prevenir acessos não autorizados.

Reposição de peças e equipamentos

Declarada a necessidade de substituição, o envio de um novo equipamento/peça/componente é realizado pelo fabricante, representante autorizado ou CONTRATADA de acordo com a tabela de Nível de serviço presente neste documento. Todos os procedimentos com o fabricante, da abertura do chamado ao seu encerramento, são de responsabilidade da CONTRATADA.

A CONTRATADA deverá realizar serviços de manutenções nos equipamentos ofertados sempre que for demandado por meio de incidentes registrados na ferramenta de Gestão de Incidentes, localizada nas dependências da Contratada.

- **Contratação de Licenciamento de Software e Serviços Agregados:**

Não é permitida a cobrança retroativa de valores referentes a serviços de suporte técnico e de atualização de versões relativa ao período em que o órgão ou entidade tenha ficado sem cobertura contratual, vedando-se cláusula direta ou indireta nesse sentido.

Não é permitida a cobrança de valores para reativação de serviços agregados, vedando-se cláusula direta ou indireta nesse sentido.

Não é permitida a cobrança de valores relativos a serviço de correção de erros, inclusive retroativos, que devem ser corrigidos sem ônus à contratante, durante o prazo de validade técnica dos softwares, nos termos do Capítulo III da Lei nº 9.609, de 19 de fevereiro de 1998. Caso os erros venham a ser corrigidos em versão posterior do software, essa versão deverá ser fornecida sem ônus para a contratante, vedando-se cláusula direta ou indireta nesse sentido.

Não é permitido exigir a contratação conjugada de serviços de suporte técnico e de atualização de versões, quando não houver a necessidade de ambos, vedando-se cláusula direta ou indireta nesse sentido.

As empresas licitantes, na proposta comercial, prestarão declaração que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio da competitividade, conforme o disposto no art. 5º da Lei nº 14.133/2021.

- **Contratação de Serviços de Manutenção e Assistência Técnica:**

A CONTRATADA deverá apresentar um plano para manutenção e suporte contínuo, incluindo detalhes sobre atualizações regulares de software e hardware, suporte técnico e resolução de problemas.

Sempre que for necessário, a CONTRATADA deverá escalonar as ocorrências e atuar em conjunto com a FABRICANTE.

A manutenção deve incluir a substituição de peças/equipamentos/componentes que possuam qualquer problema que comprometa seu perfeito funcionamento, entre eles: vícios de projeto, problemas de fabricação, construção e montagem, entre outros, sem qualquer ônus para a CONTRATANTE.

Em caso de substituição, o equipamento/peça/componente deverá ser novo e possuir configuração igual ou equivalente ao substituído, atendendo, no mínimo, às especificações constantes nos requisitos de arquitetura tecnológica deste documento.

Acesso às atualizações de correções de software (patches), melhorias do produto (updates) e mudanças de versão (upgrades).

Em relação ao atendimento remoto:

➢ Atendimento Remoto, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, em português em primeiro nível, com suporte de profissionais capacitados, que documentem o ambiente da CONTRATADA, assim como as informações, facilitando o entendimento da topologia e problemas.

- Orientações sobre uso, configuração, instalação do equipamento e implementação de funcionalidades.

- Questões sobre compatibilidade e interoperabilidade do produto instalado (hardware e software).

- Interpretação da documentação do software instalado.

- Auxílio para identificar a causa de uma falha.

- Auxílio quanto a implementação das melhores práticas sugeridas pelo fabricante em relação aos equipamentos instalados.

- Auxílio nos processos de substituição de equipamento defeituoso.

- Auxílio no processo de avaliação de capacidade e performance dos equipamentos instalados.

A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos, durante o período do contrato, para correção de problemas relativos ao uso e aplicações dos equipamentos, software e suas funcionalidades.

O atendimento aos chamados pode ocorrer remotamente ou de forma presencial. Atendimentos de severidade Alta ou Média deverão ser feitos de forma presencial quando a CONTRATANTE assim solicitar.

A CONTRATADA deverá disponibilizar técnico capacitado para execução de atividades de forma presencial nas dependências da CONTRATANTE, quando esta entender ser necessário, para atendimento aos produtos e serviços do escopo deste documento. Como exemplos, atividades que possam causar *"brick"* (inutilização de equipamento) ou que tenha um tempo de indisponibilidade que causem suspensão de prazo processual.

- **Contratação de serviços contínuos com dedicação exclusiva de mão de obra:**

Não se aplica, considerando que o item de operação e sustentação de solução não caracteriza mão de obra exclusiva.

- **Níveis de Serviço:**

Os níveis mínimos de serviço esperados para esta contratação, bem como para os atendimentos aos incidentes/eventos associados estão indicados na Tabela - Níveis Mínimos de Serviço.

Todos os prazos para a resolução dos incidentes/eventos especificados na Tabela - Níveis Mínimos de Serviço são contados a partir da abertura (registro) do chamado.

A abertura do chamado com fornecimento do seu número de identificação (protocolo de atendimento) a partir da tentativa de contato pela CONTRATANTE com o número fornecido pela CONTRATADA deve ocorrer no prazo máximo de

- 30 (trinta) minutos, se Severidade Alta ou Média.
- 60 minutos, se Severidade Baixa.

O Prazo de Resolução do problema dar-se-á a partir do registro do chamado, seja de forma automática, pela ferramenta da CONTRATADA, ou pela CONTRATANTE.

Para atendimentos presenciais, o tempo de deslocamento do funcionário da CONTRATADA será considerado dentro do prazo de resolução do incidente.

A severidade deve levar em conta o fator que foi usado na sua abertura e seguir esse mesmo critério até a sua completa solução. O chamado poderá ser reclassificado pela CONTRATANTE de acordo com a criticidade do problema.

A expressão “dia útil” refere-se ao período das 9h às 19h, de segunda a sexta-feira, excluindo-se feriados que venham a coincidir com este período.

SEVERIDADE	CLASSIFICAÇÃO	TEMPO DE ATENDIMENTO	PRAZO DE RESOLUÇÃO
(A) Alta	São consideradas como “ALTA” todas as falhas cujas consequências tenham impactos negativos e severos, gerando indisponibilidade sobre o serviço e o tráfego e/ou recursos. São situações que exijam atenção imediata. Exemplo: Situação de indisponibilidade total do equipamento, funcionamento intermitente ou parcial do equipamento, que possa levar à interrupção intermitente ou total de serviços ou perda de tráfego.	O prazo para início do atendimento após registro formal da ocorrência será de 30 minutos.	4,5 horas corridas com solução definitiva ou aplicação de medida de contorno que permita estabilização do ambiente para posterior solução definitiva.
(B) Média	Problemas que não prejudicam significativamente o funcionamento dos sistemas/serviços dos equipamentos. São problemas sérios ou perturbações, que afetam uma área específica ou determinada funcionalidade do equipamento.	O prazo para início do atendimento após registro formal da ocorrência será de 30 minutos.	O prazo para atendimento com solução definitiva ou de contorno será de 8,5 horas corridas.

SEVERIDADE	CLASSIFICAÇÃO	TEMPO DE ATENDIMENTO	PRAZO DE RESOLUÇÃO
	Configurações emergenciais para atender requisitos do negócio serão classificadas como média. Exemplo: Perda de redundância, reinicialização de módulos, slots ou portas com defeitos, degradação de desempenho, perda de funcionalidades, bloqueios de tráfego indevidos, criação ou ajuste de políticas para atender demandas inesperadas...		
(C) Baixa	Solicitação de informações sobre o funcionamento dos equipamentos, possíveis configurações ou usos, que não gerem interrupções, nem indisponibilidade de determinada área ou uma funcionalidade específica.	O prazo para início do atendimento após registro formal da ocorrência será de 60 minutos.	O prazo para atendimento com solução definitiva ou de contorno será de 48 horas corridas

Serão aceitos para atendimento e cumprimento dos prazos acima indicados o suporte direto do fabricante, sem o direito de isenção de responsabilidade pela CONTRATADA.

A CONTRATADA não será penalizada para incidentes em que a causa do problema seja comprovadamente externa a sua infraestrutura (exemplo: indisponibilidade total do switch *core* da rede da CONTRATADA), mas deverá apresentar solução de contorno que dentro das possibilidades da solução.

Caso os prazos não sejam cumpridos, a CONTRATADA sofrerá as devidas sanções previstas na legislação vigente.

Caso os prazos não sejam cumpridos, a CONTRATADA sofrerá as devidas sanções previstas na legislação vigente.

Para os casos que a causa-raiz necessite de troca do equipamento, total ou parcial, o chamado do incidente será colocado em “espera” até a reposição da peça. Neste caso, o prazo para resolução do incidente será suspenso e será retomado após a reposição ter sido concluída. Um novo chamado será aberto relacionado à troca, total ou parcial, e será utilizada a diretriz de “*SLA para reposição de peças/equipamentos*” citados logo abaixo.

SLA PARA REPOSIÇÃO DE PEÇAS/EQUIPAMENTO

Os módulos e peças de reposição devem ser novos, idênticos às originais ou de qualidade superior, homologadas pelo do fabricante e de qualidade e características iguais ou equivalentes aos dos componentes defeituosos.

SEVERIDADE	CLASSIFICAÇÃO	TEMPO DE ATENDIMENTO	PRAZO DE RESOLUÇÃO
(A) Alta	São consideradas como "ALTA" todas as falhas cujas consequências tenham impactos negativos e severos, gerando indisponibilidade sobre o serviço e o tráfego e/ou recursos. São situações que exijam atenção imediata. Exemplo: Situação de indisponibilidade total da solução, funcionamento intermitente do equipamento que prejudique funcionamento do ambiente e impossibilite solução de contorno.	O prazo para início do atendimento após registro formal da ocorrência será de 30 minutos.	4 horas corridas com solução definitiva ou aplicação de medida de contorno que permita estabilização do ambiente para posterior solução definitiva.
(B) Média	Problemas que não prejudicam significativamente o funcionamento dos sistemas/serviços do equipamento. São problemas sérios ou perturbações, que afetam uma área específica ou determinada funcionalidade do equipamento. Exemplos: Perda de um equipamento, sendo a estrutura mantida pela disponibilidade (nó passivo), perda de um módulo que que possa ser remanejado ou parada de uma das fontes redundantes.	O prazo para início do atendimento após registro formal da ocorrência será de 30 minutos.	O prazo para atendimento com solução definitiva será de até três dias úteis.
(C) Baixa	Perdas menores que não causem impacto no ambiente. Exemplo: Porta inoperante que não é utilizada	O prazo para início do atendimento após registro formal da ocorrência será de 60 minutos.	O prazo para atendimento com solução definitiva será de cinco dias úteis.

Deve ser entendida como "reposição" (processo conhecido no mercado como "RMA") a entrega do equipamento de substituição em modalidade de acordo com a planilha acima.

A CONTRATADA não será penalizada para incidentes em que a causa do problema seja comprovadamente externa a sua infraestrutura (exemplo: falha elétrica

da rede da CONTRATADA), mas deverá apresentar solução de contorno que dentro das possibilidades da solução.

O reparo no equipamento deverá ser realizado em data e horário autorizados pela CONTRATANTE.

Critérios de Aceitação:

Critérios de Aceitação:

1.1.1. A avaliação da execução do objeto contratual utilizará o Instrumento de Medição de Resultado (IMR), conforme descrito neste item. Este instrumento define, de forma objetiva, tangível e verificável, os níveis esperados de qualidade da prestação dos serviços e as respectivas adequações de pagamento, em conformidade com as boas práticas definidas pelo Guia de Contratações de TIC do Poder Judiciário e as disposições das Instruções Normativas SGD/ME nº 94/2022 e SEGES/ME nº 98/2022.

1.1.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94/2022, a CONTRATANTE poderá efetuar a retenção ou glosa no pagamento, proporcionalmente à irregularidade verificada, nos casos em que a CONTRATADA:

1.1.2.1. Não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação.

1.1.2.2. Não produzir os resultados esperados ou deixar de executar as atividades contratadas.

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

1.1.2.4. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

1.1.3. A CONTRATADA deverá ter seu desempenho avaliado com base nos critérios de Níveis de Serviço e Serviço de Operação e Sustentação, estabelecidos neste Termo de Referência.

1.1.3.1. Para esta contratação, a prestação de serviço mensal da CONTRATADA refere-se apenas ao Serviço de Operação e Sustentação, cujo pagamento será mensal.

1.1.3.2. O acompanhamento do atendimento dos Níveis de Serviço também será alvo da fiscalização de contrato, porém, em caso de descumprimento, serão encaminhados pelos fiscais e gestor do contrato à área competente para avaliação das sanções cabíveis.

1.1.4. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

IAP – ÍNDICE DE ATENDIMENTO NO PRAZO	
Tópico	Descrição
Finalidade	Medir a frequência do técnico da CONTRATADA que realizar as visitas mensais.
Meta a cumprir	IAP igual ou superior a 95%.
Instrumento de medição	Será aferido por meio de relatório emitido pela CONTRATANTE e assinada por ambas as partes. O relatório deverá conter data da visita, horário de início e fim, descrição das atividades executadas no ambiente.
Forma de acompanhamento	Será apurado mensalmente pelos fiscais do contrato, que avaliarão a frequência das visitas, além da coerência das atividades descritas dentro do relatório de atividades e efetividade das soluções propostas.
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	IAP = 100 * (ΣQtap / ΣQtr) Onde: IAP = Indicador de atendimento aos prazos do serviço; ΣQtap = Somatório do quantitativo de horas de prestação de serviço para o período de referência; ΣQtr = Somatório do quantitativo total contratado (64 horas) para o período de referência.
Observações	Obs1: Serão utilizadas horas corridas na medição.

	Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.
Faixas de ajuste no pagamento e Sanções	IAP >= 95%: sem descontos sobre o valor da fatura mensal. IAP >= 85% e < 95%: 10% de desconto sobre o valor da fatura mensal. IAP >= 75% e < 85%: 20% de desconto sobre o valor da fatura mensal. IAP < 75%: 30% de desconto sobre o valor da fatura mensal.

- **Exigências de Habilitação:**

- **Qualificação técnico-operacional:**

Comprovação de aptidão para a prestação dos serviços similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

Para fins da comprovação de que trata o subitem anterior, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas, consideradas similares às do serviço que se pretende contratar:

Fornecimento de equipamentos NGFW.

Serviço de implantação das funcionalidades IPSEC VPN, SSL VPN, Firewall e Threat Prevention/Detection (com pelo menos IPS e antivírus/antimalware).

Será admitido, para fins de comprovação de quantitativo mínimo, o somatório de atestados.

Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da empresa licitante.

O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, entre outros documentos.

Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

A apresentação de certidões ou atestados de desempenho anterior emitido em favor de consórcio do qual tenha feito parte será admitido, desde que atendidos os requisitos do art. 67, §§ 10 e 11, da Lei nº 14.133/2021 e regulamentos sobre o tema.

Qualificação técnico-profissional: Não se aplica .

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

- **Requisitos Legais:**

O presente processo de contratação deve estar aderente à Constituição Federal, Lei 14.133/21, à Resolução CNJ nº 468/2022, à Instrução Normativa SGD/ME nº 94/2022, no que não conflitar com a regulamentação do Poder Judiciário, à Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Resolução CNJ n.º 370/2021, Resolução CJF n.º 477/2018 e a outras legislações aplicáveis.

Resolução PRES nº 294, de 19 de agosto de 2019 - Implanta a Instrução Normativa 37-06, que trata da Política de Segurança de Tecnologia da Informação da Justiça Federal da 3.ª Região.

Decreto nº 7.174/2010: Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireta da União;

O não parcelamento da contratação ampara-se no Acórdão nº 1099/2008 - TCU Plenário, e em que houve manifestação quanto ao entendimento de que, havendo dependência entre os serviços que compõem o objeto licitado, a opção pelo não parcelamento mostra-se adequada, no mínimo do ponto de vista técnico; . (LEI nº 14.133/2021, Art 18. INCISO VIII)

PDTI (Plano Diretor de Tecnologia da Informação) TRF3, em que as contratações de Tecnologia da Informação no âmbito da JF3R levam em consideração esse certame para que funcionalidades e/ou ferramentas idênticas não sejam adquiridas. (LEI nº 14.133/2021, Art 18. INCISO XI)

Manual de Fiscalização de contratos da Justiça Federal e a Resolução 580 sobre as regras de atuação que devem ser seguidas quanto a fiscalização . (LEI nº 14.133/2021, Art 18. INCISO X)

Nota Técnica nº 02/2008 - SEFTI/TCU - Estabelece o uso do pregão para aquisição de bens e serviços de tecnologia da informação;

- **Requisitos Sociais, Ambientais e Culturais:**

Esse requisito será detalhado nos critérios de sustentabilidade.

- **Vistoria:**

Para TRF3 e SJSP, A vistoria prévia às instalações da CONTRATANTE é facultativa, podendo ser agendada até o horário do pregão com o Sr. Eduardo Antônio Raga Luccas – Seção de Administração de Armazenamento e Data Centers – RADC, através do telefone (11) 3012-1836/1028 ou, preferencialmente, através do endereço eletrônico radc@trf3.jus.br. Adicionalmente, o Sr. Leonardo Ponzetto – Divisão De

Infraestrutura E Conectividade – DINC, poderá ser acionado para esse agendamento no telefone 3012-1683 ou, preferencialmente, através do endereço eletrônico dinc@trf3.jus.br.

Para o TRF2: A vistoria prévia às instalações da CONTRATANTE é facultativa, podendo ser agendada até o horário do pregão com o Sr. Marcus Vinícius Azevedo – Divisão de Serviços de Rede e Mensagens – DIREM, através do telefone (21)2282-8367 ou, preferencialmente, através do endereço eletrônico direm@trf2.jus.br. Adicionalmente, o Sr. Pergentino Joaquim Alves Neto – Subsecretaria de Infraestrutura de TI – SITI, poderá ser acionado para esse agendamento no telefone (21)2282-8078 ou, preferencialmente, através do endereço eletrônico siti@trf2.jus.br.

Para a SJES: A vistoria prévia às instalações da CONTRATANTE é facultativa, podendo ser agendada até o horário do pregão com o Supervisor da Seção de Redes de Computadores (SERED), ou seu substituto eventual, através do telefone (27) 3183-5045 ou, preferencialmente, através do endereço eletrônico sered@jfes.jus.br.

Para o TRF4: A vistoria prévia às instalações da CONTRATANTE é facultativa, podendo ser agendada até o horário do pregão com o Sr. Henrique Cassol – Diretor da Secretaria de Infraestrutura e Tecnologia, através do telefone 51 3213 3611 ou, preferencialmente, através do endereço eletrônico stec@trf4.jus.br.

Para a SJSC: A vistoria prévia às instalações da CONTRATANTE é facultativa, podendo ser agendada até o horário do pregão com o Sr. Rafael Augusto da Silva - diretor do Núcleo de Infraestrutura e Segurança de TI, através do telefone 48 3251 2969 ou, preferencialmente, através do endereço eletrônico dti.seguranca@jfsc.jus.br. Adicionalmente, o Sr. Rogério Abreu da Cunha - diretor da Divisão de Tecnologia da Informação, poderá ser acionado para esse agendamento no telefone 48 99128 9570 ou, preferencialmente, através do endereço eletrônico dti.direcao@jfsc.jus.br.

Para a SJRS: A vistoria prévia às instalações da CONTRATANTE é facultativa, podendo ser agendada até o horário do pregão com o Sr. Alexandre da Silveira Ilha, Supervisor da Seção de Segurança da Informação, do Núcleo de Infraestrutura e Segurança, através do telefone +55 (51) 3214.9064 ou, preferencialmente, através do endereço eletrônico cinfra-l@jfrs.jus.br. Adicionalmente, o Sr. Igor Alexandre Dutra e Silva - Supervisor da Seção de Gerenciamento de Datacenter, do Núcleo de Infraestrutura e Segurança, poderá ser acionado para esse

agendamento no telefone +55 (51) 3214.9064 ou, preferencialmente, através do endereço eletrônico cinfra-l@jfrs.jus.br.

Para o TRF1: A vistoria prévia às instalações da CONTRATANTE é facultativa, podendo ser agendada até o horário do pregão com o Sr. Renato Solimar Alves – Supervisor da Seção da Informação Digital, através do telefone 61 3314-1695/ 1906 ou, preferencialmente, através do endereço eletrônico ditec@trf1.jus.br. Adicionalmente, o Sr. Luiz Alberto Lima da Costa – Diretor da Divisão de Tecnologia, poderá ser acionado para esse agendamento no telefone 61 3314-1695/ 1906 ou, preferencialmente, através do endereço eletrônico ditec@trf1.jus.br.

Para a SJDF: A vistoria prévia às instalações da CONTRATANTE é facultativa, podendo ser agendada até o horário do pregão com o Sr. Wellington Andrade Prudêncio – Encarregado do Setor de Tecnologia de Redes e Infraestrutura, através do telefone 61 3321-6314/ ou, preferencialmente, através do endereço eletrônico settec.df@trf1.jus.br. Adicionalmente, o Sr. João Victor de Araujo Figueiredo, poderá ser acionado para esse agendamento no telefone 61 3221-6317/ ou, preferencialmente, através do endereço eletrônico settec.df@trf1.jus.br.

Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia, devendo ocorrer até a data e horário da realização da licitação.

Para a vistoria, o representante legal da empresa ou o responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

- **Sustentabilidade:**

O licitante provisoriamente classificado em primeiro lugar deverá apresentar juntamente com a proposta comprovação de que os bens ofertados não contêm substâncias perigosas em concentração acima da recomendada na diretiva RoHS

(Guia Nacional de Contratações Sustentáveis - 4ª Edição, revista, atualizada, ampliada - agosto 2021 - Advocacia Geral da União (AGU).

Vale destacar que é impossível identificar no ETP todos os materiais recicláveis possíveis de serem utilizados nas embalagens dos equipamentos, pois há muitos tipos e formas de materiais recicláveis. É comum que os equipamentos venham embalados em caixas de papelão ou papel, mas no interior estejam acondicionados em embalagens de isopor e plástico, sendo os referidos materiais também recicláveis e podem ser admitidos como critérios de sustentabilidade. Desse modo, prever apenas um tipo de material sem atentar para as diversidades de mercado poderá comprometer a competitividade do certame.

- **Indicação de Marcas ou Modelos:**

Na presente contratação não haverá a indicação de marcas ou modelos.

- **Vedação de Marcas ou Modelos:**

Não há vedação de marcas ou modelos.

- **Subcontratação:**

É permitida a subcontratação parcial do objeto, nas seguintes condições:

- Serviço de implantação com mão de obra certificada pelo Fabricante, em que a empresa é qualificada pelo Fabricante para serviços de implantação.

- Suporte técnico oficial do FABRICANTE, para os chamados de últimos níveis.

- Serviço agregado de operação e sustentação, em que o profissional é qualificado pelo Fabricante.

- Serviço de treinamento da equipe técnica, em que o centro de treinamento é certificado pelo FABRICANTE da solução.

A comprovação de qualificação dar-se-á através de documento emitido pelo Fabricante da solução.

Justificativa: A comprovação acima garante que ao Centro de Treinamento forneça um serviço oficial e homologado pela fabricante, aderente à solução contratada. Destaca-se que é a principal solução de segurança, sendo a mais crítica para um ambiente tecnológico.

É vedada a subcontratação completa ou da parcela principal do objeto da contratação, a qual consiste em:

- Gerenciamento do projeto de implantação.

- Fornecimento dos equipamentos. Os equipamentos devem ser faturados pela CONTRATADA.

- Suporte técnico de primeiro nível.

O contrato oferece maior detalhamento das regras que serão aplicadas em relação à subcontratação.

Participação de pessoas físicas:

Devido à complexidade da Contratação envolvendo aquisição de equipamentos de segurança, mão-de-obra especializada, garantia estendida para serviços e bens e serviço agregado de operação e sustentação de ambiente não é possível que pessoas físicas participem do processo.

Participação de cooperativas:

Devido à complexidade e à necessidade de disponibilidade de aquisição da solução completa, suporte técnico contínuo, garantia estendida mais a contratação de serviço agregado para operação e sustentação da mesma solução, a execução do objeto requer uma estrutura organizacional e administrativa robusta, com disponibilidade para prestar a implementação e os serviços de forma ininterrupta e integrada.
Considerando que as cooperativas são caracterizadas por uma estrutura de gestão e operacional diferenciada, não necessariamente voltada à especialização e ao fornecimento de suporte técnico e garantia para equipamentos de rede complexos, conclui-se que a participação de cooperativas não atende de forma plena e satisfatória às especificidades técnicas e administrativas requeridas para a execução do objeto deste Termo de Referência.

Participação de consórcios:

Considerando a especificidade técnica do objeto, que demanda alto grau de especialização, acesso direto ao suporte e atualizações do FABRICANTE, bem como a necessidade de uma gestão contratual centralizada, a formação de consórcios pode introduzir complexidades adicionais na gestão do contrato.

A natureza do serviço, que compreende suporte técnico especializado, suporte técnico e garantia bens e serviços de rede de alta performance, exige uma interlocução direta e eficiente entre a CONTRATANTE e a CONTRATADA, podendo a divisão de responsabilidades intraconsórcios comprometer a agilidade e a eficácia na resolução de problemas e no atendimento das demandas.

Ademais, consórcios não são usuais, no caso específico, pelas empresas que fornecem esse tipo de manutenção e suporte, haja vista que as mesmas são concorrentes no mercado. Como não se trata de solução de alta complexidade, entendemos que a referida contratação não se enquadra no Acórdão TCU 2.831/2012-Plenário.

Portanto, para garantir a homogeneidade do serviço, o controle qualidade, e a rapidez na comunicação e atendimento, opta-se por vedar a participação de consórcios.

Participação de ME/EPP/Equiparadas:

Não é adequada a participação exclusiva de ME /EPP considerando o valor da contratação acima de R$ 80.000,00.

- **Adoção do Sistema de Registro de Preços (SRP):**

.Considerando as necessidades Tribunal Regional Federal da 3ª Região e demais órgãos coparticipes mencionados, opta-se pela adoção do Sistema de Registro de Preços (SRP) para a presente. Esta decisão encontra fundamento no art. 3º do Decreto nº 11.462/2023, , inciso III quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas; que regulamenta o SRP, permitindo a aquisição

A implementação do SRP será processada mediante LICITAÇÃO na modalidade de PREGÃO ELETRÔNICO, em conformidade com os critérios definidos para esta modalidade, Esta escolha baseia-se na eficiência, na agilidade e na competitividade promovidas pelo pregão eletrônico, permitindo a obtenção das melhores propostas com transparência e publicidade.

Considera-se a possibilidade de prorrogação da vigência da ata de registro de preços para o período de um ano adicional, conforme previsão legal e orientação do Decreto nº 11.462/2023, art. 22, desde que comprovada a vantagem econômica para a JF3R, tendo em vista a natureza dos serviços que podem apresentar demandas contínuas ao longo do tempo.

- **Compra Compartilhada com outros Órgãos:**

A presente contratação será uma compra compartilhada com outros órgãos, através do instrumento de ata de registro de preço (ARP). O TRF3 será o órgão gerenciador da ARP, sendo os coparticipes os SJSP, TRF2,SJES , TRF4, SJSC, SJDF , SJRS e TRF1.

- **Adesão a Ata de Registro de Preços - ARP:**

Seguirá as regras descritas pelo Decreto 11.462, em especial o seguinte: conforme art. 22. Do decreto 11.462, “O prazo de vigência da ata de registro de preços será de um ano, contado do primeiro dia útil subsequente à data de divulgação no PNCP, e poderá ser prorrogado por igual período, desde que comprovado que o preço é vantajoso.”

“Será autorizado a adesão à Ata conforme prevê o art. 30 da Resolução CJF n° 842/2023 c/c o art. 86, § 2º, da Lei 14.133/2021 e o art. 7º, XI, do Decreto 11.462/2023, considerando o quantitativo conforme art. 32, incisos I e II do Decreto 11.462/2023.”

O TRF3 será o órgão gerenciador da ata de registro de preço.

- **Exigência de Amostra, Exame de Conformidade ou Prova de Conceito:**

Não se há necessidade técnica para solicitar amostra, exame de conformidade ou prova de conceito considerando todas as medidas de segurança para a implantação da solução.

- **Utilização de mão de obra, materiais, tecnologias e matérias-primas existentes no local da execução, conservação e operação do bem ou serviço:**

A CONTRATADA utilizará o rack, pontos lógicos e pontos elétricos da CONTRATANTE para a instalação dos equipamentos da solução.

Acessos internos serão providos pela CONTRATANTE como usuários, VPNs, ponto de rede etc.

- **Catálogo de Soluções de TIC com Condições Padronizadas:**

Esta solução não se enquadra nos itens do Catálogo de Soluções de TIC.

- **Matriz de risco**

Não foi incluída matriz de risco devido ao valor da contratação não ser de grande vulto previsto no art. 6º inciso XXII da Lei nº 14.133/2021.

2. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

GRUPO 1								
ITEM	ESPECIFICAÇÃO	MÉTRICA UNIDADE DE MEDIDA	CATMAT CATSER	CÓD PMC-TI	TRF3 QTD.	SJSP QTD.	TRF2 QTD.	SJES QTD.
1	Appliance de Firewalls NGFW	Equipamento	609340	-	2	2	4	2
2	Licenciamento para os recursos dos Firewalls NGFW Internos	Licença	27502	-	1	1	0	-
3	Licenciamento para os recursos dos Firewalls NGFW Externos (incluso 1000 usuários SSL VPN	Licença	27502	-	1	1	4	2

	(client-to-site) e 500 VPN IPSec site-to-site)							
4	Firewall de contingência	Equipamento	609340	-	1	1	0	-
5	Licenciamento para os recursos dos Firewalls NGFW de Contingência	Licença	27502	-	1	1	0	-
6	Gerência da solução de firewall	Equipamento	481647	-	1	1	1	1
7	Serviço de Implantação	Serviço	27090	-	3	3	4	2
8	Treinamento técnico	Vouchers	27740	-	10	0	4	4
9	Serviço de Operação e Sustentação de Solução por 60 meses	Serviço	27090	-	1	0	1	1

ITEM	ESPECIFICAÇÃO	MÉTRICA UNIDADE DE MEDIDA	CAT MAT CAT SER	CÓD. PMC-TI	TRF4 QTD.	SJSC QTD.	SJRS QTD.	TRF1	SJDF QTD
1	Appliance de Firewalls NGFW	Equipamento	609340	-	4	2	2	4	
2	Licenciamento para os recursos dos Firewalls NGFW Internos	Licença	27502	-	2	2	-	2	
3	Licenciamento para os recursos dos Firewalls NGFW Externos (incluso 1000 usuários SSL VPN (client-to-site) e 500 VPN IPSec site-to-site)	Licença	27502	-	2	2	2	2	
4	Firewall de contingência	Equipamento	609340	-	-	-	-	-	2
5	Licenciamento para os recursos dos Firewalls NGFW de Contingência	Licença	27502	-	-	-	-	-	2
6	Gerência da solução de firewall	Equipamento	481647	-	1	1	1	1	1
7	Serviço de Implantação	Serviço	27090	-	4	2	2	4	2
8	Treinamento técnico	Vouchers	27740	-	5	3	6	6	4
9	Serviço de Operação e Sustentação de Solução por 60 meses	Serviço	27090	-	1	1	1	1	1

Item 1

- Especificação: Appliance de Firewalls NGFW
- Motivação Técnica: Necessidade de nova solução de segurança do tipo firewall na infraestrutura do TRF3. Esse ativo é um item essencial e crítico para qualquer organização no quesito segurança da informação.
- Quantitativos:
    - Estimativa: 22 equipamentos (total)
    - Metodologia de Cálculo: Desenho da solução implica na necessidade de 4 equipamentos, conforme figura 1.

Item 2

- Especificação: Licenciamento para os recursos dos Firewalls NGFW Internos
- Motivação Técnica: O funcionamento pleno das ferramentas da solução principal depende de licenças do tipo permanente para habilitar os recursos solicitados.
- Quantitativos:
    - Estimativa: 8 conjuntos de licenças, sendo uma por equipamento. (total)
    - Metodologia de Cálculo: 1 conjunto de licenças para cada appliance da solução principal interna.

Item 3

- Especificação: Licenciamento para os recursos dos Firewalls NGFW Internos (incluso 1000 usuários SSL VPN (client-to-site) e 500 VPN IPSec site-to-site)
- Motivação Técnica: O funcionamento pleno das ferramentas da solução principal depende de licenças do tipo permanente para habilitar os recursos solicitados.
- Quantitativos:
    - Estimativa: 16 conjuntos de licenças, sendo uma por equipamento. (total)
    - Metodologia de Cálculo: 1 conjunto de licenças para cada appliance da solução principal externa.

Item 4

- Especificação: Firewall de contingência
- Motivação Técnica: Necessidade de um acesso remoto a infraestrutura de modo independente em caso de um desastre.
- Quantitativos:
    - Estimativa: 4 equipamentos (total)
    - Metodologia de Cálculo: Questão de redundância, conforme apresentado na Figura 2.

Item 5

- Especificação: Licenciamento para os recursos dos Firewalls NGFW de Contingência
- Motivação Técnica: O funcionamento pleno das ferramentas da solução de contingência depende de licenças do tipo permanente para habilitar os recursos solicitados.
- Quantitativos:
    - Estimativa: 4 conjuntos de licenças, sendo uma por equipamento. (total)
    - Metodologia de Cálculo: 1 conjunto de licenças para cada appliance da solução de contingência.

Item 6

- Especificação: Gerência da solução de firewall
- Motivação Técnica: A gerência é uma forma de centralizar a operação e manutenção de toda solução de forma simplificada.
- Quantitativos:
    - Estimativa: 9 equipamentos (total)
    - Metodologia de Cálculo: Questão de redundância e boas práticas, principalmente para appliance físico. Uma solução instalada em cada site da CONTRATADA.

Item 7

- Especificação: Serviços de Implantação por conjunto equipamento-licença

- Motivação Técnica: Necessidade de mão de obra especializada para implantação dos equipamentos. Por ser um equipamento crítico e de implantação delicada é necessária a contratação desse serviço.
- Quantitativos:
    - Estimativa: 26 serviços (total)
    - Metodologia de Cálculo: Quantidade de equipamentos a serem implantados.

Item 8

- Especificação: Treinamento técnico
- Motivação Técnica: A equipe técnica da CONTRATANTE deverá ser capacitada adequadamente para operar a solução.
- Quantitativos:
    - Estimativa: 40 vouchers de treinamento. (total)
    - Metodologia de Cálculo: A equipe técnica conta com 5 (cinco) servidores. Porém, a subsecretaria UARI solicitou registrar preço para participantes adicionais, contemplando a DINC (1), UARI (1), SETI (1), eventual posse de novos servidores (2). Portanto, iremos registrar preço do treinamento na solução para um total de 10 participantes para o TRF3.
    - Para os demais os demais órgãos, vide detalhamento na tabela do item 2 deste documento.

Item 9

- Especificação: Serviço de Operação e Sustentação de Ambiente
- Motivação Técnica: por ser uma nova solução com uma drástica mudança na infraestrutura interna e pela necessidade de uma resposta mais célere a incidentes, contrataremos um especialista na solução vencedora.
- Quantitativos:
    - Estimativa: 60 meses (o mesmo valor para cada órgão participante da ATP)

- Metodologia de Cálculo: De acordo com o novo escopo de projeto e de acordo com o prazo de extensão de garantia.
- A justificativa da demanda dos órgãos copartícipes constam no DOP sei 0004918-44.2024.4.03.8000

3. ANÁLISE DE SOLUÇÕES POSSÍVEIS

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

3.1. Identificação das Soluções:

SOLUÇÃO	DESCRIÇÃO DA SOLUÇÃO
1	Soluções baseadas exclusivamente em software open source
2	Solução oferecida como serviço.
3	Aquisição de solução proprietária.
4	Renovação de suporte técnico e garantia da solução atual.

3.2. Análise Comparativa Técnica de Soluções:

- **Solução 1: Software Open Source**

Soluções em software livre, são um tipo de software onde o código-fonte está disponível para todos que quiserem usar. Ele é construído, assim como sua manutenção, de maneira colaborativa. Dessa forma, qualquer pessoa pode investigar, alterar e redistribuí-lo. O *open source* beneficia diferentes iniciativas, pois não está focado em obter lucros relacionados à propriedade intelectual.

São soluções que costumam não ter custos com licenças ou relacionados a propriedade intelectual, logo, em termos financeiros, costumam ter seu custo reduzido ao comparar com uma solução proprietária. Destaca-se que empresas podem utilizá-los como base para comerciar um produto, cobrando por subscrições de atualizações de bases, correções etc.

São disponibilizados no formato de software, sendo agnósticos a qualquer tipo de hardware.

Por terem seu código-fonte livre, é possível que seja realizada diversas customizações no software para atender requisitos específicos da instituição.

Dependendo da aplicação, é possível contar com o auxílio de outros desenvolvedores e de uma comunidade voltada para aquela ferramenta.

- **Solução 2: Serviço**

A utilização de contratação de serviço, ou terceirização da gestão, é uma modalidade a qual a empresa realiza uma assinatura, com pagamento mensal ou anual.

Assim, não há responsabilidade técnica por parte da equipe interna pois todas as funções relacionadas ao gerenciamento, manutenção e aquisição de equipamentos ficam a cargo da empresa contratada.

A contratada realiza todas as atividades técnicas como configuração, manutenção, backup, melhorias e resolução de problema. Os chamados internos relacionados a alterações no firewall também ficam a cargo da empresa.

Este tipo de serviço pode ser adquirido em diversas formas a fim de atender as demandas da CONTRATANTE.

Geralmente, há uma equipe totalmente especializada no assunto para operar a solução e realizar um atendimento satisfatório. Esse atendimento pode ser tanto em dias comerciais, como na modalidade 24x7x365.

A contratante também não precisa se preocupar em aquisição de equipamentos para substituição ou treinamentos regulares para equipe interna.

- **Solução 3: Proprietário**

Solução proprietária é aquela à qual é desenvolvida por uma empresa a qual detém o direito sobre aquele conjunto de ferramentas.

Para ter acesso de uso, de forma legal, é necessário comprar uma licença ou subscrição.

Esse tipo de solução geralmente conta com o apoio e suporte do fabricante em casos de ajuda, bugs ou outras necessidades. São ferramentas que são conhecidas pelo mercado e há uma boa oferta de profissionais que entendem e dão suporte ou treinamento mediante a um contrato de serviço.

Nessa modalidade, a equipe interna de uma empresa pode passar por um treinamento fornecido pela fabricante ou um terceiro homologado.

Geralmente são ofertados em forma de appliance físico ou virtual. Em ambos os casos, a contratante terá algum nível de suporte da fabricante durante o período que a licença estiver ativa.

É usual que esse tipo de solução seja utilizado por empresas que porte grande devido a ter um respaldo direto do fabricante.

- **Solução 4: Renovação de suporte técnico e garantia da solução atual**

Como já discorrido, a solução atual entrará em end-of-life pelo fabricante em janeiro de 2027.

O equipamento atual é uma solução Cisco Firepower Serie 4110. Essa solução renovaria a garantia até o período máximo possível pelo fabricante.

4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Inicialmente, temos que levar em consideração a figura abaixo a qual auxiliou a equipe técnica para desenhar a arquitetura.

O "quadrante mágico"[2] demonstra quais são os melhores firewalls de mercado atualmente.

O quadrante é lido da seguinte maneira, sendo do melhor para o menos hábil: Leaders (Líderes), Challengers (Desafiantes), Nich Players (Empresas de Nichos), Visionaries (Visionários).

FIGURA 3- QUADRANTE MÁGICO PARA FIREWALLS[3]

- **Solução Inviável : Soluções baseadas exclusivamente em software open source (Solução 1)**

Não foram consideradas uma vez que (a) necessitam de investimento em infraestrutura (aquisição de equipamentos, sistemas operacionais etc.), (b) exigem também, no caso de software pago, a manutenção de contratos de subscrição para atualização de software e das bibliotecas de assinatura de código malicioso, quando contemplam esta funcionalidade, (c) exigem, no caso de software livre, a designação

[2] *https://www.gartner.com/en/research/magic-quadrant*

[3] *https://www.fortinet.com/content/dam/fortinet/images/diagrams/diagram-gartner-network-firewalls1.png*

de equipe de segurança dedicada e especializada e investimentos em processos contínuos de capacitação, (d) impõem restrições à alta disponibilidade e à prestação de suporte adequado e tempestivo, além de (e) não implementarem todos os requisitos de segurança de porte corporativo, de forma ampla e efetiva.

Por sua vez, também não foram encontradas soluções de firewall que estivesse nos dois primeiros quadrantes do Gartner.

- **Solução Inviável – Solução oferecidas como serviço (Solução 2)**

Não foram consideradas, pois promovem a transferência de domínio dos recursos de segurança a terceiros e é competência da Administração a salvaguarda dos ativos de informação. Não obstante, por se tratar de um ativo extremamente crítico que necessita de atendimento mais célere, logo, o tempo de atendimento é um requisito importante.

A experiência do TRF3 em solução de TI oferecidas como serviço demonstrou que o tempo de atendimento das CONTRATADAS tende a ser mais elevado do que o esperado, e, em muitas vezes, houve prejuízo na boa prestação.

- **Solução Inviável – Renovação de Suporte Técnico e Garantia de NGFW Cisco Firepower (Solução 4)**

A renovação do serviço até a data supracitada não está sendo cogitada, visto que seria uma aquisição não vantajosa para a Administração, pelos seguintes motivos: (a) tempo a ser utilizado bem inferior a cinco (5) anos; (b) solução que está se tornando obsoleta e; (c) necessidade de reduzir a complexidade do cenário atual e (d) ausência de funcionalidade de utilização de wildcards em camada de aplicação.

5. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

5.1. Cálculo dos Custos Totais de Propriedade

- **Solução Viável 1: Aquisição de solução proprietária (Solução 3)**

○ Memória de Cálculo de Custos Totais de Propriedade:

ITEM	ESPECIFICAÇÃO	MÉTRICA UNIDADE DE MEDIDA	TOTAL QTD.	VALOR UNITÁRIO ESTIMADO	VALOR TOTAL ESTIMADO
1	Appliance de Firewalls NGFW	Equipamento	22	R$ 265.398,87	R$ 5.838.775,14
2	Licenciamento para os recursos dos Firewalls NGFW Internos	Licença	8	R$ 3.534.169,75	R$ 28.273.358,00
3	Licenciamento para os recursos dos Firewalls NGFW Externos (incluso 1000 usuários SSL VPN (client-to-site) e 500 VPN IPSec site-to-site)	Licença	16	R$ 3.534.169,75	R$ 56.546.716,00
4	Firewall de contingência	Equipamento	4	R$ 27.518,77	R$ 110.075,08
5	Licenciamento para os recursos dos Firewalls NGFW de Contingência	Licença	4	R$ 98.183,18	R$ 392.732,72
6	Gerência da solução de firewall	Equipamento	9	R$ 111.024,26	R$ 999.218,34
7	Serviço de Implantação	Serviço	26	R$ 49.815,84	R$ 1.295.211,84
8	Treinamento técnico	Vouchers	42	R$ 16.500,00	R$ 693.000,00
9	Serviço de Operação e Sustentação de Solução por 60 meses	Serviço	8	R$ 136.433,33	R$1.091.466,64
VALOR TOTAL	R$ 95.240.553,76				

5.2. Mapa comparativo dos cálculos totais de propriedade (TCO)

O único item que será pago em 5 anos é o item 9 .Mensal estimado em R$ 2.273,88.

6. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

A solução a ser escolhida por esse Tribunal é a solução proprietária com suporte do fabricante.

A equipe interna já tem ampla experiência com esse formato e tem se mostrado assertivo.

A solução escolhida envolve solução completa de firewall (aquisição de equipamentos, implantação e treinamento) com adição de garantia estendida para serviço (suporte técnico) e bens (hardware) e serviço agregado de operação e sustentação de ambiente com mão de obra especialista.

A solução envolve seis firewalls, os quais trabalharão em pares: um par de NGFW internos, um par de NGFW externo e um par de NGFW de contingência. Junto com esses seis dispositivos teremos mais um par de software que fará toda a gerência e administração. Para que a solução funcione a contento, serão adquiridas licenças que atenderão todos os itens do tópico “Arquitetura Tecnológica”.

Os pares de firewalls terão funções distintas, sendo que o classificado como “Interno” tratará de tráfego interno entre as redes de usuário e servidores. Por outro lado, o firewall “externo” tratará de acessos das redes supracitadas para as redes de “DMZ”, VPN (cliente e Site-to-site) e internet, independente se a origem são DMZ ou VPN/Internet.

Por fim, há um par de NGFW de menor porte o qual recebeu o nome de “Firewall de contingência”. O intuito desse dispositivo é estar presente para garantir um acesso independente em uma eventual situação de desastre que impeça o acesso a infraestrutura externamente pelos modos convencionais. Por esse motivo, ele será um equipamento com recursos mais limitados e direcionado para que a equipe técnica da CONTRATANTE consiga acesso e faça o trabalho de “*troubleshooting*”, a fim de resolver o problema crítico.

7. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Tendo em vista o Item 5 – Análise Comparativa de Custos, diante da solução Viável 1, tem-se que o custo total estimado da contratação R$ R$ 95.240.553,76.

8. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Esta equipe de planejamento declara viável esta contratação, sob o aspecto técnico, socioeconômico e ambiental.

A equipe de planejamento, analisando a contratação pretendida, diante de todo o exposto nos itens anteriores deste Estudo Técnico Preliminar, considera a solução acima apontadas como as mais viáveis tecnicamente e economicamente para atender as necessidades de segurança da Justiça Federal da 3ª Região, trazendo os seguintes benefícios:

- Mitigação de indisponibilidades, pois o equipamento terá garantia estendida para bens e serviços pelo prazo de 60 meses.
- Maior confiabilidade e robustez, pois o equipamento possui tecnologia mais modernas e aptas a aguentar a carga de trabalho dos equipamentos presentes no data center e dos usuários da Justiça Federal da 3ª Região.
- Maior desempenho, há mais interfaces disponíveis e um backplane mais robusto.
- Maior granularidade nas políticas a serem criadas e aplicadas.
- Melhor flexibilidade na operação do equipamento, com a possibilidade de trabalhar com regras mais dinâmicas em camada 7.

Por fim, destacamos que este documento pode ser classificado como público, nos termos da inciso I do artigo 28 e parágrafo único da Resolução CNJ nº 468/2022 e artigo 17 da Resolução PRES nº 587/2023.

9. APROVAÇÃO E ASSINATURA

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO		
Integrante Técnico	**Integrante Demandante**	**Autoridade Máxima de TI**
GUILHERME JORGE EGASHIRA:3821 Assinado de forma digital por GUILHERME JORGE EGASHIRA:3821 Dados: 2024.09.25 16:59:57 -03'00'		DANIEL HENRIQUE GUIMARAES:3624 Assinado de forma digital por DANIEL HENRIQUE GUIMARAES:3624 Dados: 2024.09.25 17:13:47 -03'00'
Integrante Administrativo	David Panessa Baccelli:2604 Assinado de forma digital por David Panessa Baccelli:2604 Dados: 2024.09.25 17:26:53 -03'00'	
Simone Sanches Alves:3311 Assinado de forma digital por Simone Sanches Alves:3311 Dados: 2024.09.25 16:55:33 -03'00'		