MALOTE DIGITAL

Tipo de documento: Administrativo

Código de rastreabilidade: 512202525974317

Nome original: 3 - Termo de Referência de STIC (TR).pdf

Data: 19/08/2025 17:16:35

Remetente:

Tecnologia da Informação

Tecnologia da Informação

Tribunal Regional do Trabalho da 12ª Região

Documento: não assinado.

Prioridade: Normal.

Motivo de envio: Para conhecimento.

Assunto: Concordância dos órgãos participantes com os Estudos Técnicos Preliminares e Termo de Referência do registro de preços para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall.

Termo de Referência de STIC (TR)[1]

Aquisição de Bens de STIC

PROAD 12629/2024
PAC ID 15021
SIGEO ID: 151132025000172

1. Unidade Demandante e Unidade Gestora de Orçamento

Unidade Demandante: Secretaria de Tecnologia da Informação e Comunicação (SETIC)

Unidade Gestora do Orçamento: Secretaria de Tecnologia da Informação e Comunicação (SETIC)

2. Descrição da Solução (Objeto)

Contratação de serviço de suporte e manutenção para solução de Next Generation Firewall, em cluster, para 60 meses, com gerenciamento centralizado e integrado, garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico 24 horas; Aquisição de equipamentos Next Gereration Firewall, com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses, Capacitação para solução de Firewall; Aquisição de solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers); Voucher de Treinamento para solução SASE e ZTNA e Contratação de serviço gerenciado mensal, conforme tabela TR1, abaixo.

Importante: Para esta contratação será adotada a definição de *cluster* como o conjunto de dois, ou mais, equipamentos *appliances* compatíveis entre si, que

[1] Em regra, conforme art. 28, da Resolução nº 468/2022, o DOD, ETP e TR serão disponibilizados em sítio eletrônico de fácil acesso e no Connect-Jus até a data de publicação do edital da licitação. A avaliação de acesso à informação contida em ETP, com informações sensíveis ou sigilosas, será analisada a critério de cada órgão do poder judiciário, respeitando os termos da Lei no 12.527/2011, e da Resolução CNJ no 215/2015.

trabalham de forma integrada e foram construídos especificamente para exercer a função de Next Generation Firewall.

Tabela TR1 - Descrição dos Grupos e Itens da contratação

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento	
Item	**Descrição**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo II - Pagamento em parcela única, antecipada.**
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em parcela única, antecipada.**
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em 5 parcelas fixas anuais.**
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em 5 parcelas fixas anuais.**
6	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo IV - Pagamento em parcela única, antecipada.**
7	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo V - Pagamento em parcela única, antecipada.**
8	Voucher de **Treinamento** para solução de proteção de perímetro de rede lógica do tipo Next Generation **Firewall**
Grupo II - Aquisição de licenciamento e equipamentos para promover conexão de rede SD-WAN via Firewall	
9	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls **Tipo I e Tipo IV**

10	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 2 e 7 - Firewalls **Tipo II e Tipo V**
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VI**
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VII**
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VIII**
Grupo III - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers) na modalidade Software como serviço e Treinamento	
14	Licença de uso de solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)** por usuário pelo período de 60 meses
15	Voucher de Treinamento para solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)**
Grupo IV - Serviço gerenciado mensal	
16	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) - **Tipo I e Tipo IV**
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) - **Tipo II e Tipo V**
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 5) - **Tipo III**
19	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) - **Tipo VI, Tipo VII e Tipo VIII**

Observação: Por se tratar de processo nacional, foi realizada reunião de alinhamento inicial e definição de requisitos para o processo, conforme registrado no documento 54 do presente processo.

Integram esta licitação desde o início, na forma do § 5º, do art. 12, da Resolução CNJ nº 468/2022, tendo enviado DOD e quantitativos, que estão anexados ao Proad nos documentos de marcadores 15 a 34 e 52, os seguintes órgãos:

Tribunal Superior do Trabalho (TST);

Tribunal Regional do Trabalho da 1ª Região (TRT1);

Tribunal Regional do Trabalho da 3ª Região (TRT3);
Tribunal Regional do Trabalho da 4ª Região (TRT4);
Tribunal Regional do Trabalho da 5ª Região (TRT5);
Tribunal Regional do Trabalho da 6ª Região (TRT6);
Tribunal Regional do Trabalho da 7ª Região (TRT7);
Tribunal Regional do Trabalho da 9ª Região (TRT9);
Tribunal Regional do Trabalho da 10ª Região (TRT10);
Tribunal Regional do Trabalho da 11ª Região (TRT11);
Tribunal Regional do Trabalho da 12ª Região (TRT12);
Tribunal Regional do Trabalho da 13ª Região (TRT13);
Tribunal Regional do Trabalho da 14ª Região (TRT14);
Tribunal Regional do Trabalho da 15ª Região (TRT15);
Tribunal Regional do Trabalho da 16ª Região (TRT16);
Tribunal Regional do Trabalho da 17ª Região (TRT17);
Tribunal Regional do Trabalho da 18ª Região (TRT18);
Tribunal Regional do Trabalho da 19ª Região (TRT19);
Tribunal Regional do Trabalho da 20ª Região (TRT20) ;
Tribunal Regional do Trabalho da 21ª Região (TRT21);
Tribunal Regional do Trabalho da 22ª Região (TRT22);
Tribunal Regional do Trabalho da 23ª Região (TRT23).

2.1 Identificar código(s) do Catmat e/ou Catser

Conforme consulta no endereço eletrônico disponível em https://catalogo.compras.gov.br/cnbs-web/, realizada em 2/7/2024.

2.1.1. Itens 1 a 5 - Suporte e Garantia a Equipamentos NG Firewall

Código CATSER: 27740
Nome do Serviço: Serviços de garantia de equipamentos de tic.

2.1.2. Itens 6, 7, 11, 12 e 13 - Equipamento NG Firewall e SD-Wan:

Código CATMAT: 609340

Aplicação: Segurança Rede Computadores
Modelo: Appliance Ngfw

2.1.3. Item 9, 10 e 14 - Licença para uso de função SD-WAN nos equipamentos NG Firewall e Licença Sase e ZTNA:

Código CATSER: 27464
Nome do Serviço: Licenciamento de direitos permanentes de uso de software para servidor.

2.1.4. Itens 16 a 19 - Operação Assistida:

Código CATSER: 27014
Nome do Serviço: Serviços de gerenciamento de infraestrutura de tecnologia da informação e comunicação (tic)

2.1.5. Itens 8 e 15 - Treinamentos

Código CATSER: 3840
Nome do Serviço: Treinamento informática - sistema / software

3. Justificativa e Fundamentação da Contratação

3.1. Motivação

Inicialmente é importante registrar que os processos trabalhistas desta justiça especializada são 100% digitais e tramitam via sistema PJe - Processo Judicial Eletrônico.

Desta forma, a prestação jurisdicional depende totalmente da rede de dados e do acesso à Internet.

Neste contexto cabe pontuar que a solução de Firewall é um pilar para as redes de dados conforme dois motivos principais, a saber:

- Para que o Firewall cumpra seu papel como barreira de segurança ele deve inspecionar todo o tráfego da rede, portanto, a melhor posição para sua configuração é fazendo o papel de roteador principal dos dados, pois assim, filtra-se todo o conteúdo que circula entre as redes da instituição, e;

- No caso específico dos Tribunais do Trabalho, a solução de Firewall ainda provê os acessos remotos seguros, essenciais para o teletrabalho e prestação de serviços remotos de contratos terceirizados.

Contextualizada a importância do Firewall e considerando o término do contrato de suporte vigente da solução atual em 2025, o que deixará os Tribunais sem suporte e sem direito à atualização da solução de Firewall. Assim, torna-se imprescindível manter a solução de NG Firewall sob suporte, garantia e atualização.

3.2. Benefícios da Contratação

- Manter operacionais as redes de dados dos Tribunal, com garantia de Níveis Mínimos de Serviço em caso de problemas;
- Garantir camada de segurança contra ataques cibernéticos para as redes de dados corporativas da JT, e;
- Viabilizar o teletrabalho no âmbito da Justiça do Trabalho.

3.3. Alinhamento Estratégico do órgão Gerenciador (TRT12)

Embora não seja um projeto estratégico, a ação está relacionada com os seguintes objetivos da estratégia do TRT/SC - 2021-2026[2]:

- Garantir a duração razoável do processo, e;
- Aprimorar a Governança de TIC e a proteção de dados.

3.4. Alinhamento ao Plano Diretor de TIC (PDTIC) do órgão Gerenciador (TRT12)

[2]O plano estratégico 2021 - 2026 do TRT12 está disponível em: https://portal.trt12.jus.br/Planejamento_Estrategico/PE_2021_2026

PDTIC TRT12 - 2025-2026:

- Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados, e;
- Objetivo 8: Promover Serviços de Infraestrutura e Soluções Corporativas.

3.5. Referência aos estudos preliminares

O documento contendo os estudos técnicos preliminares atualizados para a contratação em tela estão contidos no PROAD 12629/2024.

3.6. Relação entre demanda prevista e quantidade contratada

O compêndio de itens com sua descrição e quantitativos definidos estão descritos na tabela TR2, abaixo. No Anexo II consta a tabela com os quantitativos a serem registrados para atender as necessidades de cada Tribunal Regional do Trabalho.

Tabela TR2 - Descrição e quantidades da demanda dos órgãos participantes

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento				
Item	**Descrição**	**Unidade (1)**	**Estimativa Mínima (2)**	**Estimativa Máxima**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**	Cluster	10	11
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de	Cluster	5	6

	administração e gerência integrada - **Tipo II - Pagamento em parcela única, antecipada.**			
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em parcela única, antecipada.**	Cluster	4	4
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em 5 parcelas fixas anuais.**	Cluster	1	1
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em 5 parcelas fixas anuais.**	Cluster	1	1
6	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo IV - Pagamento em parcela única, antecipada.**	Cluster	1	1
7	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo V - Pagamento em parcela única, antecipada.**	Cluster	3	4
8	Voucher de **Treinamento** para solução de proteção de perímetro de rede lógica do tipo Next Generation **Firewall**	Aluno	38	100
Grupo II - Aquisição de licenciamento e equipamentos para promover conexão de rede SD-WAN via Firewall				
9	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls **Tipo I e Tipo IV**	Licença / Cluster	3	3
10	Licenciamento de Serviço de Software-Defined WAN	Licença	2	3

	(SD-WAN) compatível com os equipamentos NGFW dos itens 2 e 7 - Firewalls **Tipo II e Tipo V**	/ Cluster		
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VI**	Equip.	2	17
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VII**	Equip.	18	68
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VIII**	Equip.	4	64
Grupo III - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers) na modalidade Software como serviço				
14	Licença de uso de solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)** por usuário pelo período de 60 meses	Usuário	3700	28200
15	Voucher de Treinamento para solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)**	Aluno	33	120
Grupo IV - Serviço gerenciado mensal				
16	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) - **Tipo I e Tipo IV**	Serviço/ Cluster	9	10
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) - **Tipo II e Tipo V**	Serviço/ Cluster	6	8
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 5) - **Tipo III**	Serviço/ Cluster	4	4
19	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em	Serviço/ Equip.	18	81

	regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) - **Tipo VI, Tipo VII e Tipo VIII**			

(1) Para esta contratação será adotada a definição de cluster como o conjunto de dois, ou mais, equipamentos appliances compatíveis entre si, que trabalham de forma integrada e foram construídos especificamente para exercer a função de Next Generation Firewall.
(2) Entende-se como estimativa mínima, especificada por Tribunal no Anexo II, a quantidade que cada participante compromete-se a solicitar a cada pedido feito.

3.7. Análise do Mercado de TIC e Soluções disponíveis

Nos Estudos Técnicos Preliminares foram analisadas três soluções sobre Firewall para a segurança de rede dos Tribunais do Trabalho, focando nas vantagens e desvantagens de cada uma. A primeira opção, Firewall como Serviço (FWaaS), propõe uma solução em nuvem gerenciada por um provedor externo. Embora ofereça escalabilidade ilimitada, manutenção simplificada e alta disponibilidade, apresenta desvantagens significativas. A latência aumenta, o que é crítico para sistemas internos, e há uma dependência direta do provedor de nuvem.

A integração com a infraestrutura local predominante ainda é essencial nos Tribunais da JT, como o TRT12, que possui Data Centers físicos, é complexa e exige reconfigurações de rede extensas, tornando essa solução inviável para a maioria dos casos.

A segunda solução considera a Aquisição de Novos Equipamentos Firewall instalados fisicamente nos Tribunais. As vantagens incluem a atualização tecnológica com novas funcionalidades e a possibilidade de redimensionar a capacidade da solução para atender às demandas futuras. Contudo, essa opção acarreta alguns riscos. A migração é complexa e pode gerar interrupções de serviço ou perda de dados. Há também a necessidade de as equipes técnicas investirem em treinamento para operar os novos sistemas, além do alto custo inicial de aquisição e instalação. Do ponto de vista da sustentabilidade é importante considerar que o descarte de equipamentos antigos gerará lixo eletrônico.

Já a solução 3, Contratação do Serviço de Suporte e Manutenção para a Solução de NG Firewall já existente, foi a escolhida. Esta solução se tornou viável devido à substituição preventiva dos equipamentos antigos (modelos 5800, 23500 e 15600) por modelos mais recentes (6700 e 16200) pela empresa NTSEC, sem custos adicionais para os Tribunais. Essa substituição atualizou a infraestrutura de

firewall, estendendo sua vida útil até 2030, e permitiu manter a solução on-premise, que continua a atender aos requisitos de desempenho. Além disso, os Firewalls Checkpoint, utilizados pela maioria dos Tribunais, estão entre os melhores do mundo, segundo o Gartner Group.

Essa escolha se alinha com princípios de sustentabilidade, pois aproveita os recursos já instalados, evitando a produção de novos equipamentos e o descarte desnecessário dos atuais. Além disso, a manutenção da infraestrutura existente elimina os riscos de migração, que poderiam causar interrupções nos sistemas ou perdas de dados. As equipes técnicas dos Tribunais já possuem um conhecimento aprofundado sobre a operação desses equipamentos, o que garante agilidade na resolução de problemas e otimização das políticas de segurança sem a necessidade de uma nova curva de aprendizado. Essa abordagem também assegura o aproveitamento máximo da vida útil dos equipamentos, maximizando o retorno sobre o investimento inicial.

Do ponto de vista financeiro e orçamentário, a Solução 3 oferece benefícios significativos. Ela possibilita uma economia de 49,03% em relação à aquisição de novos equipamentos do Tipo I (comparação do valor estimado para os itens 1 e 4) e de 38,5% em relação à aquisição de novos equipamentos do Tipo III (comparação do valor estimado para os itens 3 e 5), conforme Estimativa de Preliminar de Preços.

Adicionalmente, essa contratação é classificada como despesa de GND3 (Serviços), e não GND4 (Investimentos), o que pode ser crucial para Tribunais com restrições orçamentárias, facilitando a aprovação e execução do contrato. A flexibilidade de pagamento, permitindo tanto o pagamento antecipado para 5 anos quanto o pagamento anual, proporciona maior adaptabilidade às condições financeiras dos órgãos, tornando a contratação viável mesmo diante de acentuadas restrições orçamentárias impostas ao Judiciário em 2025.

4. Especificação completa da solução escolhida

Devida a complexidade das especificações completas da solução, para evitar erros materiais e facilitar a leitura tanto deste documento, quanto do documento com as especificações completas, as informações referentes à esta seção estarão disponíveis em anexos, conforme segue:

- Anexo I - Especificações Técnicas para Solução de Next Generation Firewall (NGFW).

5. Sustentabilidade

Os bens adquiridos via Itens 6, 7, 11, 12 e 13 não devem conter substâncias nocivas ao meio ambiente tais como mercúrio, chumbo, cromo hexavalente, cádmio, bifenil-polibromados, éteres difenil-polibromados, em concentração acima da recomendada pela Diretiva 2002/95/EC do Parlamento Europeu também conhecida como diretiva RoHS (Restriction of Certain Hazardous Substances).

O pregoeiro solicitará ao Licitante provisoriamente classificado em primeiro lugar que apresente ou envie juntamente com a proposta, sob pena de não-aceitação, comprovação de que o bem ofertado não contém substâncias perigosas em concentração acima da recomendada na diretiva RoHS.

A comprovação poderá ser feita, alternativamente, mediante apresentação de certificação RoHS, Rótulo Ecológico da ABNT, Epeat, certificação emitida por organismo acreditado pelo INMETRO, certificação emitida por instituição pública oficial ou instituição/empresa certificadora, laudo pericial, folheto técnico, declaração de conformidade emitida pela fabricante, manual do produto, ou consulta on-line no site da fabricante, devendo a licitante fornecer o site para consulta, que atestem que o objeto fornecido cumpre com as exigências do edital.

Todo o material técnico originalmente elaborado em língua estrangeira deverá ser acompanhado de tradução em língua portuguesa.

Para os demais itens não foram identificados requisitos relacionados à sustentabilidade.

6. Nível Mínimo de Serviço

Cabe relembrar que os serviços dos Itens 1 a 5, Serviço de garantia e atualização de assinaturas de proteção e suporte técnico, e o mesmo serviço vinculado às aquisições dos Itens 6, 7, 11, 12 e 13 não garantem níveis mínimos de serviço, conforme explicação do item 6.5 do ETP.

Desta forma, o serviço gerenciado de Firewall é crucial para assegurar a disponibilidade dos sistemas de TIC e a integridade dos dados digitais, pois garante a resolução de problemas e aprimoramentos da solução dentro de níveis mínimos de serviço previstos em contrato. Além disso, supre a carência de mão de obra técnica especializada, oferecendo uma operação assistida 24x7 com atendimento proativo para incidentes relacionados ao Firewall.

Seguem os Níveis Mínimos de Serviço aplicáveis ao Grupo IV (Itens 16 a 19), seguem no documento Anexo I - Especificações Técnicas para Solução de Next Generation Firewall - NGFW, item 4.3. Nível Mínimo de Serviço Para o Grupo IV - Serviço gerenciado mensal para equipamentos Firewall (Itens 16 a 19).

7. Obrigações e Responsabilidades da Contratada

A Contratada se obriga a:

a) Observar e cumprir, estritamente, as condições ora estabelecidas, obedecendo a critérios e prazos acordados pelas exigências técnicas constantes do edital deste contrato;

b) Durante toda a execução do contrato, manter-se, em conformidade com as obrigações assumidas, atendendo a todas as condições de habilitação e qualificação exigidas na licitação;

c) Prestar todos os esclarecimentos que forem solicitados pelo responsável da fiscalização do contrato;

d) Proceder, no início da contratação, ao seu cadastramento no SIGEO-JT - Sistema Integrado de Gestão Orçamentária e Financeira da Justiça do Trabalho - Módulo Execução Orçamentária, bem como responsabilizar-se pela gestão de seus dados;

e) Responsabilizar-se pela juntada, por meio do referido Sistema, dos documentos de cobrança/documentos fiscais (notas fiscais/faturas);

f) Observar e cumprir, estritamente, os termos da proposta e as condições ora estabelecidas, obedecendo a critérios e prazos acordados pelas exigências técnicas constantes do edital e contrato;

g) Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

i. Manter a regularidade fiscal e trabalhista durante todo o período contratual, sob pena de rescisão contratual e de execução da retenção sobre os créditos da empresa e/ou da eventual garantia, a título de multa, para ressarcimento dos valores e indenizações devidos à Administração, além das penalidades previstas em lei;

ii. Se for Optante pelo Simples Nacional deverá apresentar a Declaração, conforme modelo constante no Anexo IV da Instrução Normativa nº 1.234/2012 da Receita Federal do Brasil, no momento da apresentação da primeira nota fiscal/fatura decorrente da assinatura do contrato ou da prorrogação contratual;

iii. Informar imediatamente qualquer alteração da sua permanência no Simples Nacional;

h) Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução do contrato, ex vi do caput do art. 121 da Lei nº 14.133/2021;

i) Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados (art. 119 da Lei 14.133/2021);

j) Manter quadro de pessoal suficiente para atendimento dos contratos, conforme previsto neste contrato e em legislação específica, sem

interrupção, seja por motivo de férias, descanso semanal, licença, greve, falta ao serviço e demissão de empregados, que não terão em hipótese alguma, qualquer relação de emprego com o Contratante;

k) Prestar todos os esclarecimentos que forem solicitados pelos responsáveis pelo acompanhamento e fiscalização da execução do contrato;

l) Fornecer crachás para seus empregados, contendo seu nome e o da Contratada, sendo obrigatório seu uso nas dependências do Contratante, nos termos da Portaria PRESI nº 311/99, art. 175, § 4º;

m) Substituir imediatamente qualquer um de seus empregados que for considerado inconveniente à boa ordem e às normas disciplinares do Contratante;

n) Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo Contratante;

o) Marcar com despesa decorrente de qualquer infração, seja de que natureza for, desde que praticada por seus empregados no recinto do Contratante;

p) Protocolizar, se necessário, as petições no Coordenadoria de Cadastramento de Recursos aos Tribunais Superiores PROTOCOLO do Contratante, situado na rua Esteves Júnior, 395, bairro Centro, na cidade de Florianópolis/SC, CEP 88015-905;

q) Atentar para as práticas de sustentabilidade na execução dos serviços nos termos do art. 6º do Capítulo III da Instrução Normativa nº 01, de 19/01/2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão;

r) Obedecer, no que couber, aos princípios e normas de conduta estabelecidas

no Código de Ética do Contratante.

s) Informar e manter atualizado endereço de e-mail válido, para comunicação oficial entre Contratante e Contratada.

t) A Contratada deverá, em até 10 dias após a comunicação da assinatura do contrato, indicar empregado para exercer o papel de Preposto, bem como seu e-mail e telefone de contato. O Preposto deve ter capacidade gerencial para tratar todos os assuntos previstos neste Termo de Referência e no instrumento contratual correspondente, sem implicar em ônus para o contratante.

u) Caso ocorra a inexecução total do contrato pela Contratada, sem prejuízo das multas e demais sanções previstas em lei, fica estabelecido que a Contratada deverá restituir integralmente o valor pago antecipadamente pelo Contratante. O valor a ser restituído deverá ser atualizado monetariamente com base no Índice de Custos de Tecnologia da Informação (ICTI), estabelecido na Portaria nº 6.432, de 11 de julho de 201829, do Ministério do Planejamento, Desenvolvimento e Gestão (ou outro índice definido pela Equipe de Planejamento da Contratação durante a elaboração deste Termo de Referência). A atualização monetária será aplicada desde a data do pagamento antecipado até a data da efetiva restituição.

v) Caso ocorra a inexecução parcial do contrato pela Contratada, sem prejuízo das multas e demais sanções previstas em lei, fica estabelecido que a Contratada deverá realizar a restituição proporcional dos valores pagos antecipadamente pelo contratante.

w) A restituição proporcional será calculada com base na porcentagem de execução dos serviços previstos no contrato. O valor a ser restituído será atualizado monetariamente com base no Índice de Custos de Tecnologia da Informação (ICTI), estabelecido na Portaria nº 6.432, de 11 de julho de 2018, do Ministério do Planejamento, Desenvolvimento e Gestão (ou outro índice definido pela EPC durante a elaboração deste Termo de Referência). A

atualização monetária será aplicada desde a data do pagamento antecipado até a data da efetiva restituição.

x) O local de prestação dos serviços/entrega dos bens constará no Anexo III.

7.1. Das obrigações da Contratada em face da LGPD

a) Para os fins da Lei Geral de Proteção de Dados (Lei n. 13.709/18), na hipótese de, em razão do presente contrato, a Contratada realizar o tratamento de dados pessoais como operadora ou controladora, deverá adotar as medidas de segurança técnicas, jurídicas e administrativas aptas a proteger tais dados pessoais de acessos não autorizados ou qualquer forma de tratamento inadequado ou ilícito, observando-se os padrões mínimos definidos pela Autoridade Nacional de Proteção de Dados em conformidade com o disposto na legislação de proteção de dados e privacidade em vigor, sem prejuízo do disposto nas alíneas subsequentes;

b) Dar tratamento aos dados pessoais a que tiver acesso por força do contrato tão-somente na medida do cumprimento do escopo contratual, vedado o tratamento para quaisquer outros propósitos;

c) Não fornecer transferir ou disponibilizar dados pessoais a terceiros, a menos que com base em instruções explícitas, por escrito, do Contratante ou por ordem de autoridade judicial, sob a condição de que, nesse último caso, informando ao Contratante dentro de 24 (vinte e quatro) horas após o recebimento da ordem judicial, ressalvadas as hipóteses legais de sigilo na investigação em que o tratamento sigiloso tenha sido expressamente exigido pela autoridade judicial, quando a Contratada estará dispensada da comunicação ao Contratante;

d) Não colocar o Contratante em situação de violação da LGPD;

e) Assegurar que seus empregados tenham ciência dos termos da LGPD, que assinem o “Termo de Confidencialidade e de Responsabilidade”, Anexo H , e que estejam capacitados para agir dentro das normas nela dispostas;

f) Assegurar que as pessoas autorizadas a tratar os dados pessoais assinem o “Termo de Confidencialidade e de Responsabilidade”, Anexo H;

g) Responsabilizar-se pelo uso indevido que seus empregados ou prestadores de serviços fizerem dos dados pessoais a que tiverem acesso pela execução contratual, bem como por quaisquer falhas nos sistemas por ela empregados para o tratamento dos dados;

h) Cessar o tratamento de dados pessoais realizado com base no Contrato imediatamente após o seu término e, a critério exclusivo do Contratante, apagar, destruir ou devolver os dados pessoais que tiver obtido;

i) Nos casos em que realizar o tratamento de dados pessoais confiados pelo Contratante, a Contratada será considerada "operadora" e deverá aderir à Política de Privacidade e Proteção de Dados do Contratante.

8. Obrigações e Responsabilidades do contratante

O Contratante se obriga a:

a) Acompanhar a execução do contrato, nos termos do art. 117 da Lei nº 14.133/21 e nos arts. 2º a 8º da Portaria PRESI nº 163/20, através dos responsáveis pelo acompanhamento e fiscalização da execução do contrato, que exercerá ampla e irrestrita fiscalização do objeto do presente contrato, a qualquer hora, determinando o que for necessário à regularização das faltas ou defeitos observados, inclusive quanto às obrigações da Contratada;

b) Proporcionar todas as facilidades necessárias à boa execução do contrato, especialmente as condições indispensáveis para o acesso seguro ao ambiente;

c) Efetuar os pagamentos devidos à Contratada, nos prazos e condições ora estabelecidos;

d) Prestar as informações e esclarecimentos que venham a ser solicitados pela Contratada.

8.2. Deveres e responsabilidades do órgão gerenciador da ata de registro de preços

O TRT 12, como órgão gerenciador, se obriga a:

a) Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

b) Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

c) A comunicação entre o Órgão Gerenciador e os órgãos participantes e não participantes, se dará por mensagens via sistema Comprasnet, na Internet, mensagens de correio eletrônico e ligações telefônicas para o órgão gerenciador, sendo o telefone e o endereço de e-mail da área técnica do órgão gerenciador os seguintes:
   - e-mail: infra@trt12.jus.br, e;
   - Telefone: (48) 3216-4125.

9. Forma da contratação

A solução objeto desta contratação possui padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado, desta forma deverá ser realizada licitação, do tipo pregão eletrônico, com o critério de menor preço, utilizando o Sistema de Registro de Preços.

O TRT12 atuará como órgão gerenciador da licitação, considerando a complexidade da contratação e a participação de 22 órgãos, a fim de permitir o gerenciamento adequado da ARP, entendemos que não deverá ser permitida a adesão de outros órgãos além daqueles que já integram esta contratação desde o início. Portanto, não deverá ser realizada a Intenção de Registro de Preços.

Em conformidade com o artigo 84 da Lei nº 14.133/2021, propõe-se que a Ata de Registro de Preços (ARP) tenha vigência de 1 (um) ano, com a possibilidade de prorrogação, inclusive dos quantitativos, por igual período, desde que demonstrada a manutenção de preços vantajosos.

A inclusão da previsão de prorrogação se justifica pelas características específicas desta ARP, que se configura como um instrumento nacional destinado a atender às necessidades de diversos órgãos. A solução abrangida pela ARP é composta por múltiplos itens, incluindo suporte e atualização, bem como aquisições de equipamentos, além de itens complementares que podem ser combinados de diversas formas.

A flexibilidade proporcionada pela prorrogação é crucial para otimizar a utilização da ARP pelos órgãos participantes. A possibilidade de solicitar itens complementares conforme a demanda e a disponibilidade orçamentária, sem a necessidade de iniciar novos processos licitatórios para cada aquisição, permite que os órgãos usufruam de forma mais completa e eficiente da solução contratada. Mantendo, inclusive a conformidade com os demais tribunais.

Adicionalmente, a prorrogação, quando economicamente vantajosa, evita a descontinuidade no fornecimento e reduz os custos administrativos associados à realização de novas licitações, contribuindo para a eficiência da gestão pública.

9.1. Parcelamento da Solução

A motivação para o parcelamento da solução consta no item 7.1 Parcelamento da Solução. Abaixo segue a divisão dos grupos. Cada grupo será tratado como um lote independente, permitindo a participação e adjudicação de um ou mais lotes a uma mesma empresa. O licitante poderá apresentar proposta para um, alguns ou todos os grupos/itens.

Tabela TR4 - Descrição dos Grupos e Itens da contratação

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento		
Item	**Descrição**	**Unidade (1)**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**	Cluster
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo II - Pagamento em parcela única, antecipada.**	Cluster
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em parcela única, antecipada.**	Cluster
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em 5 parcelas fixas anuais.**	Cluster
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em 5 parcelas fixas anuais.**	Cluster
6	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo IV - Pagamento em parcela única, antecipada.**	Cluster
7	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo V - Pagamento em parcela única, antecipada.**	Cluster
8	Voucher de **Treinamento** para solução de proteção de perímetro de rede lógica do tipo Next Generation **Firewall**	Aluno
Grupo II - Aquisição de licenciamento e equipamentos para promover conexão de rede SD-WAN via Firewall		
9	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls **Tipo I e Tipo IV**	Licença/ Cluster

10	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 2 e 7 - Firewalls **Tipo II e Tipo V**	Licença/ Cluster
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VI**	Equip.
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VII**	Equip.
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VIII**	Equip.
Grupo III - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers) na modalidade Software como serviço e Treinamento		
14	Licença de uso de solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)** por usuário pelo período de 60 meses	Usuário
15	Voucher de Treinamento para solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)**	Aluno
Grupo IV - Serviço gerenciado mensal		
16	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) - **Tipo I e Tipo IV**	Serviço/ Cluster
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) - **Tipo II e Tipo V**	Serviço/ Cluster
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 5) - **Tipo III**	Serviço/ Cluster
19	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) - **Tipo VI, Tipo VII e Tipo VIII**	Serviço/ Equip.

(1) Para esta contratação será adotada a definição de cluster como o conjunto de dois, ou mais, equipamentos appliances compatíveis entre si, que trabalham de forma integrada e foram construídos especificamente para exercer a função de Next Generation Firewall.

10. Forma e Critérios de seleção do fornecedor

Devido ao grande vulto da contratação, e a necessidade de estrutura mínima, com equipamentos, instalações e equipe de profissionais e corpo técnico para a execução do objeto, não será permitida a participação de pessoa física.

Considerando a necessidade de apenas um fornecedor para todos os itens de um mesmo grupo, o critério de seleção será o menor preço total para o grupo, considerando as quantidades estimadas para cada item.

É permitida a subcontratação para a execução do objeto para os seguintes itens:

a) Elaboração do projeto de implantação.
b) Instalação da solução de TIC.
c) Visitas preventivas e atendimento técnico de garantia.
d) Treinamento.

De qualque forma, permanece a responsabilidade integral do contratado pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades do subcontratado, bem como responder perante o contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

A subcontratação depende de autorização prévia do contratante, a quem incumbe avaliar se o subcontratado cumpre os requisitos de qualificação técnica necessários para a execução do objeto.

O contratado apresentará à Administração documentação que comprove a capacidade técnica do subcontratado, que será avaliada e juntada aos autos do processo correspondente.

Salientamos que a licitante deverá respeitar tanto o valor máximo estimado para cada item, quanto o valor máximo estimado para o Grupo. Os valores Máximos estimados constam neste TR e são provenientes do documento Estimativa Preliminar de Preços.

A validade da proposta deverá ser de, no mínimo, 60 dias.

Juntamente com a proposta, as empresas licitantes deverão:

a) Declarar a não ocorrência do registro de oportunidade, de modo a garantir o princípio da isonomia e a seleção da proposta mais vantajosa para a Administração Pública.

a) Para os grupos 1, 2 e 4: apresentar comprovação de que é empresa parceira (partner) do fabricante da solução com qualificação técnica e comercial para vender, implementar e manter a solução ofertada.

Ainda são necessárias as seguintes comprovações:

a) Certificado ou Comprovação de Registro Cadastral de fornecedor junto a órgãos ou entidades da Administração Pública;

b) CRF - Certificado de Regularidade do FGTS, emitido pela CEF;

c) Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União, emitida em conjunto pela Secretaria da Receita Federal e Procuradoria-Geral da Fazenda Nacional;

d) CNDT - Certidão Negativa de Débitos Trabalhistas, emitida pela Justiça do Trabalho;

e) Prova de regularidade para com a Fazenda Estadual do domicílio ou sede do licitante;

f) Prova de regularidade para com a Fazenda Municipal do domicílio ou sede do licitante;

g) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores, e;

h) Inscrição do ato constitutivo, no caso de sociedade civil, acompanhada de prova de diretoria em exercício.

Em todos os casos:

Será verificada pelo Selic no Portal da Transparência do Governo Federal, no Portal do Conselho Nacional de Justiça (CNJ) e no Sistema de Cadastramento Unificado de Fornecedores do Governo Federal (SICAF), a existência de sanções administrativas que impeçam o licitante de contratar com a administração pública.

10.1 Qualificação técnica

A exigência de capacidade técnica 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 os órgãos 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 contratante 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.

a) As empresas participantes deverão apresentar 1 (um) ou mais Atestado(s) de Capacidade Técnica distintos, emitido por pessoa jurídica de direito público ou privado, comprovando ter fornecido equipamentos e serviços similares aos descritos na tabela abaixo.

Tabela TR9 - Atestados de Capacidade Técnica

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento

Item	Descrição	Qtd. Mínima
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I**	36 meses de serviço para ao menos cinco clusters similares
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo II**	36 meses de serviço para ao menos dois clusters similares
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III**	36 meses de serviço para ao menos dois clusters similares
8	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo V**	Fornecimento de ao menos 2 equipamentos similares
Grupo II - Aquisição de licenciamento e equipamentos para promover conexão de rede SD-WAN via Firewall		
10	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 7 - Firewalls **Tipo I e Tipo IV**	Fornecimento de ao menos 1 licenciamento similar
11	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 2, 5 e 8 - Firewalls **Tipo II e Tipo V**	Fornecimento de ao menos 1 licenciamento similar
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VI**	Fornecimento de ao menos 8 equipamentos similares
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VII**	Fornecimento de ao menos 34 equipamentos similares
14	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VIII**	Fornecimento de ao menos 32 equipamentos similares
Grupo III - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers) na modalidade Software como serviço		
15	Licença de uso de solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers) por usuário pelo período de 60 meses	Fornecimento de ao menos 2000 licenças similares

Grupo IV - Serviço gerenciado mensal		
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 7) - **Tipo I e Tipo IV**	36 meses de serviço para ao menos cinco clusters similares
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2, 5 e 8) - **Tipo II e Tipo V**	36 meses de serviço para ao menos quatro clusters similares
19	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 6) - **Tipo III**	36 meses de serviço para ao menos dois clusters similares
20	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 12, 13 e 14) - **Tipo VI, Tipo VII e Tipo VIII**	36 meses de serviço para ao menos 40 clusters similares

(1) Para esta contratação será adotada a definição de cluster como o conjunto de dois, ou mais, equipamentos appliances compatíveis entre si, que trabalham de forma integrada e foram construídos especificamente para exercer a função de Next Generation Firewall.

b) 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.

10.2 Qualificação dos Profissionais

10.2.1. Para o Grupo I - itens 6 e 7

A fim de garantir a instalação dos equipamentos, a empresa contratada deve comprovar até a data de assinatura do contrato que o profissional responsável pela instalação dos equipamentos tem capacidade técnica para realização do serviço, essa comprovação se dará por certificação emitida pela própria fabricante do equipamento ou por empresa de treinamento reconhecida pelo fabricante. A

comprovação poderá ser feita por meio de certificado de participação em treinamento ou carta emitida pela fabricante do produto.

10.2.2. Para o Grupo IV - itens 16 a 19 - Serviço Gerenciado

A empresa contratada deve comprovar até a data de assinatura do contrato que dispõe, no mínimo, de profissionais com a documentação abaixo relacionada, como condição para a formalização do contrato, obrigando-se a manter-se na mesma condição durante toda a vigência do pacto decorrente da Ata de Registro de Preços.

a) Quatro profissionais com certificados expedidos pelo próprio fabricante Check Point, ou parceiro credenciado, no treinamento Check Point Security Administration (CCSA);
b) Três profissionais com certificados expedidos pelo próprio fabricante Check Point, ou parceiro credenciado, no treinamento Check Point Security Expert (CCSE);
c) Dois profissionais com certificados expedidos pelo próprio fabricante Check Point, ou parceiro credenciado, no treinamento Check Point Certified Troubleshooting Administrator (CCTA), e;
d) Dois profissionais com certificados expedidos pelo próprio fabricante Check Point, ou parceiro credenciado, no treinamento Check Point Certified Troubleshooting Expert (CCTE).

Para a comprovação das certificações, deverá ser apresentada cópia do certificado emitido pelo órgão certificador.

A contratada deverá apresentar ao menos um profissional para cada certificação e um mesmo profissional poderá atender a mais de uma certificação.

10.3 Qualificação Econômico-Financeira

A habilitação econômico-financeira visa a demonstrar a aptidão econômica do licitante para cumprir as obrigações decorrentes do futuro contrato, devendo ser comprovada de forma objetiva da seguinte forma:

I - balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais;

II - certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante.

Os documentos mencionados acima deverão comprovar as seguintes condições:

- Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

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

Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

11. Modelo de Gestão e Fiscalização do Contrato

11.1. Atribuições do Gestor do contrato

a) gerir a execução do ajuste;

b) acompanhar as ações de fiscalização;

c) diligenciar junto à empresa nos casos em que lhe forem solicitados pelo fiscal;

d) realizar o recebimento definitivo, e;

e) ao final do contrato emitir o Termo de Encerramento de Contrato.

11.2. Atribuições dos fiscais do contrato

a) Inteirar-se dos termos do contrato, gerenciar minuciosamente o cumprimento dos níveis de serviço e atentar para os prazos contratuais (prazo de início de serviço, prazo para entrega do material, para a execução do serviço, etc.);

b) Promover as ações necessárias para regularização das faltas ou defeitos observados na execução contratual, com objetivo de que ocorra nos termos acordados;

c) Eventuais decisões e providências que ultrapassarem suas competências deverão ser solicitadas ao gestor em tempo hábil para a adoção das medidas convenientes.

11.3. Atribuições do fiscal administrativo

a) Deverá realizar, mensalmente, os seguintes exames, que deverão estar anotados no Termo de Conformidade para Pagamento da Nota Fiscal:
i. comprovante de regularidade fiscal, constatada via consulta “on-line” ao Sistema de Cadastramento Unificado de Fornecedores (SICAF) e no Cadastro de Empresas Inidôneas e Suspensas - CEIS;
ii. verificar se as condições de pagamento do contrato foram obedecidas e o valor cobrado corresponde àquilo que foi fornecido (de acordo com as informações do Termo de Recebimento Provisório e medição dos Níveis Mínimos de Serviços);

b) Quanto ao recebimento dos bens adquiridos, o fiscal administrativo deve verificar a regularidade fiscal da contratada e a observância dos prazos para entrega dos bens;

c) Emitir o Atestado de Conformidade para Pagamento da Nota Fiscal (Anexo D e Anexo E), e;

d) Ao final do contrato emitir o Termo Final de Conformidade (Anexo G).

11. 4. Atribuições do fiscal demandante

a) verificar se a execução do contrato obedece aos critérios funcionais estabelecidos, devendo apresentar manifestação no processo da contratação sempre que entender necessário, para eventual correção de inconsistências verificadas.

11.5. Atribuições do fiscal técnico

a) realizar verificação dos seguintes aspectos;

b) os resultados alcançados em relação ao contrato, com a verificação do prazo de execução da qualidade demandada;

c) qualidade e quantidade dos recursos utilizados;

d) adequação dos serviços prestados à rotina de execução estabelecida;

e) adequação do bem entregue às especificações estabelecidas, e;

f) realizar o de recebimento provisório.

12. Recebimento do objeto

12.1 Recebimento Provisório de Bens (Itens 6, 7, 11, 12 e 13)

O recebimento provisório será realizado pelo Fiscal Técnico.

O fiscal técnico irá realizar o recebimento provisório, atestando a entrega dos bens adquiridos no Termo de Recebimento Provisório, de acordo com o modelo constante no Anexo A.

Nesse documento, o fiscal deve realizar o registro, a análise e a conclusão acerca das condições do material entregue, deve realizar, ainda, a conferência da

Nota Fiscal com a Nota de Empenho registrando a data da entrega e demais observações conforme modelo.

Existindo ocorrências pendentes ou que configurem descumprimento parcial do contrato, o recebimento do objeto deve ser atestado com ressalvas. Em caso de descumprimento total do contrato, o recebimento do objeto não deve ser atestado, devendo, neste caso, o Fiscal informar a ocorrência no processo para análise pelo Gestor.

O Termo de Recebimento Provisório, com ou sem ressalvas, deve ser encaminhado ao gestor do contrato, junto com outros documentos que entender necessários para esclarecer/comprovar os fatos apresentados.

12.2 Recebimento Provisório de Serviços (Itens 1, 2, 3, 4, 5, 8, 9, 10, 14, 15, 16, 17, 18 e 19)

A tabela abaixo especifica a periodicidade do recebimento provisório e definitivo de cada um dos itens de serviço.

Tabela TR10 - Periodicidade do recebimento provisório e definitivo

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento		
Item	**Descrição**	**Periodicidade**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento único e antecipado - Pagamento em parcela única, antecipada.**	Único
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo II - Pagamento em parcela única, antecipada.**	Único
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em parcela única, antecipada.**	Único

4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em 5 parcelas fixas anuais.**	Anual
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em 5 parcelas fixas anuais.**	Anual
8	Voucher de **Treinamento** para solução de proteção de perímetro de rede lógica do tipo Next Generation **Firewall**	Único
Grupo II - Aquisição de licenciamento e equipamentos para promover conexão de rede SD-WAN via Firewall		
9	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls **Tipo I e Tipo IV**	Único
10	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 2 e 7 - Firewalls **Tipo II e Tipo V**	Único
Grupo III - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers) na modalidade Software como serviço e Treinamento		
14	Licença de uso de solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)** por usuário pelo período de 60 meses	Mensal
15	Voucher de Treinamento para solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)**	Único
Grupo IV - Serviço gerenciado mensal		
16	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) - **Tipo I e Tipo IV**	Mensal
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) - **Tipo II e Tipo V**	Mensal
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 5) - **Tipo III**	Mensal
19	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) - **Tipo VI, Tipo VII e Tipo VIII**	Mensal

O fiscal técnico irá realizar o recebimento provisório, atestando a prestação do serviço no Termo de Recebimento Provisório, de acordo com o modelo constante no Anexo B.

Nesse documento, o fiscal deve realizar o registro, a análise e a conclusão acerca das ocorrências na execução do contrato no período em referência e poderá encaminhar, junto com o Termo de Recebimento Provisório, outros documentos que entender necessários para esclarecer/comprovar os fatos apresentados.

Existindo ocorrências pendentes ou que configurem descumprimento parcial do contrato, o recebimento do objeto deve ser atestado com ressalvas. Em caso de descumprimento total do contrato, o recebimento do objeto não deve ser atestado, devendo, neste caso, o Fiscal informar a ocorrência no processo para análise pelo Gestor.

No caso de serviços continuados com pagamento mensal, o recebimento provisório deverá ocorrer mensalmente, ainda que com ressalvas.

Para os itens 16 a 19 o recebimento provisório ocorrerá sempre após a conferência do Relatório emitido pela Contratada. Para estes mesmos itens, no momento do recebimento provisório, o fiscal técnico apresentará as medições dos níveis mínimos de serviços, registrando-as em relatório juntado ao PROAD da contratação.

O Termo de Recebimento Provisório, com ou sem ressalvas, deve ser encaminhado ao gestor do contrato, junto com os demais documentos, inclusive o relatório de medição de NMS, quando previstos.

12.3 Recebimento Definitivo de Bens (Itens 6, 7,11, 12 e 13)

O recebimento definitivo constitui o ato de aceitação do material, o que se dá com a verificação da qualidade e quantidade, o atendimento das especificações de acordo com o contrato, com o edital e com a proposta da contratada, quando couber, deve ser realizado pelo gestor do contrato ou por comissão nomeada para este fim, de acordo com regulamentação específica sobre administração de materiais e compras. O recebimento definitivo ocorrerá com a mesma periodicidade do recebimento provisório.

No TRT12, conforme a Portaria PRESI no 769/2022, o recebimento de material de valor superior a 10 (dez) vezes o limite estabelecido no inciso II do art. 75 da Lei no 14.133/2021 deverá ser confiado a uma comissão de, no mínimo, 3 (três) membros.

Para realizar o recebimento definitivo, o gestor do contrato ou comissão devem:

a) verificar se os materiais estão em conformidade com a descrição na respectiva nota de empenho e contrato (se houver);

b) verificar se os testes realizados com os materiais e bens atendem ao solicitado/adquirido;

c) verificar se os materiais estão em perfeitas condições de uso;

d) verificar se a Nota Fiscal está de acordo com a Nota de Empenho em relação às descrições, unidades, quantidades e valores unitários e total dos materiais;

e) registrar a data do recebimento definitivo e assinaturas do gestor ou da comissão e as demais observações que julgar pertinentes, e;

f) emitir termo próprio de recebimento definitivo dos bens fornecidos, com base nos relatórios e documentação apresentados.

O modelo de termo de recebimento definitivo a ser utilizado é o que consta no Anexo C.

Quando não aceito o material entregue, o gestor ou a comissão providenciará junto à contratada a sua regularização, sem prejuízo do registro formal em processo próprio e da contagem dos prazos para entrega efetiva do material previstos no processo de aquisição.

Verificada alguma ocorrência que possa autorizar penalização da contratada, o gestor deve realizar o recebimento definitivo do material, ainda que com ressalvas, e encaminhar o processo à apreciação superior para análise dos efeitos quanto a pagamento e abertura de processo administrativo.

O gestor deve inserir o Termo de Recebimento Definitivo no PROAD, promover o aceite da Nota Fiscal no SIGEO e encaminhar o expediente para pagamento. A nota fiscal deverá ser inserida no SIGEO pelo fornecedor.

12.4 Recebimento Definitivo de Serviços (Itens 1, 2, 3, 4, 5, 8, 9, 10, 14, 15, 16, 17, 18 e 19)

O recebimento definitivo constitui o ato que reconhece a execução dos serviços e deve ser realizado pelo gestor do contrato. O recebimento definitivo ocorrerá com a mesma periodicidade do recebimento provisório.

No caso de serviços continuados com pagamento mensal, o recebimento definitivo deverá ocorrer mensalmente, ainda que com ressalvas.

Para realizar o recebimento definitivo, o gestor deve:

a) realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à contratada, por escrito, as respectivas correções;
b) caso o contrato preveja Instrumento de Medição de Resultados (IMR), caberá ao gestor, com base no relatório apresentado pelo fiscal do contrato, analisar se o desempenho e a qualidade do serviço prestado estão em consonância com os níveis mínimos e realizar o redimensionamento de valores a serem pagos, caso constatada alguma inconformidade, pela aplicação de fator redutor;
c) emitir termo próprio para efeito de recebimento definitivo dos serviços prestados (Anexo B), com base nos relatórios e na documentação apresentados, e;
d) comunicar à contratada para que emita a nota fiscal ou fatura com o valor exato dimensionado pela fiscalização com base no IMR, quando for o caso.

O modelo de termo de recebimento definitivo a ser utilizado é o que consta no contrato, na forma apresentada no planejamento da contratação.

Verificada alguma ocorrência no período correspondente aos serviços atestados que possa autorizar penalização da contratada, o gestor deve realizar o recebimento definitivo, ainda que com ressalvas, e encaminhar o processo à

apreciação superior para análise dos efeitos quanto a pagamento e abertura de processo administrativo.

O gestor deve inserir o Termo de Recebimento Definitivo no PROAD, promover o aceite da Nota Fiscal no SIGEO e encaminhar o expediente para pagamento. A nota fiscal deverá ser inserida no SIGEO pelo fornecedor.

13. Condições de Pagamento

A tabela abaixo especifica a periodicidade do pagamento de cada um dos itens de serviço.

Tabela TR11 - Periodicidade do pagamento

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento		
Item	**Descrição**	**Periodicidade**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento único e antecipado - Pagamento em parcela única, antecipada.**	Único
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo II - Pagamento em parcela única, antecipada.**	Único
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em parcela única, antecipada.**	Único
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em 5 parcelas fixas anuais.**	Anual
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em 5 parcelas fixas anuais.**	Anual

6	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo IV - Pagamento em parcela única, antecipada.**	Único
7	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo V - Pagamento em parcela única, antecipada.**	Único
8	Voucher de **Treinamento** para solução de proteção de perímetro de rede lógica do tipo Next Generation **Firewall**	Único
Grupo II - Aquisição de licenciamento e equipamentos para promover conexão de rede SD-WAN via Firewall		
9	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls **Tipo I e Tipo IV**	Único
10	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 2 e 7 - Firewalls **Tipo II e Tipo V**	Único
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VI**	Único
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VII**	Único
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VIII**	Único
Grupo III - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers) na modalidade Software como serviço e Treinamento		
14	Licença de uso de solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)** por usuário pelo período de 60 meses	Mensal
15	Voucher de Treinamento para solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)**	Único
Grupo IV - Serviço gerenciado mensal		
16	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) - **Tipo I e Tipo IV**	Mensal

17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) - **Tipo II e Tipo V**	Mensal
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 5) - **Tipo III**	Mensal
19	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) - **Tipo VI, Tipo VII e Tipo VIII**	Mensal

Os itens 1 a 7 e 9 a 13 possuem pagamento antecipado, pois esta condição é o padrão de mercado, conforme podemos verificar tanto pelos contratos passados (Proad 11926/2017 e 9665/2023), quanto pelos contratos atuais de outros órgãos, a exemplo do TRT2 (marcador XXX).

O Acórdão 276/02 – 1ª Câmara do TCU estabelece que o pagamento antecipado é permitido em situações específicas:

- Se for condição indispensável para adquirir um bem ou serviço, ou se gerar economia substancial.
- Se houver previsão expressa em edital de licitação ou instrumentos de contratação direta.
- Mediante a adoção de cautelas e garantias indispensáveis.

O padrão da indústria para os serviços de garantia e atualização de assinaturas, conforme confirmado pelo fabricante no documento XXX, é o pagamento único e antecipado para 60 meses de cobertura. O pagamento antecipado é o padrão, entretanto, devido às restrições orçamentárias enfrentadas pelos Tribunais, foi aventada a possibilidade de pagamentos antecipados mas em cinco parcelas fixas anuais.

Embora os pagamentos anuais sejam uma opção, eles introduzem custos adicionais. Isso ocorre porque os parceiros do fabricante, e não o fabricante em si, assumem a responsabilidade financeira de adquirir a garantia de 60 meses antecipadamente e, em seguida, parcelar esses pagamentos para os tribunais.

Naturalmente, esses parceiros repassam os custos e riscos associados a esse financiamento de múltiplos anos.

Segue na tabela TR11 a comparação dos valores estimados para pagamento do serviço de suporte e garantia único e antecipado e para pagamento antecipado em cinco parcelas fixas anuais.

Tabela TR11 - Comparativo entre o pagamento único e em cinco parcelas fixas anuais

Equipamento	Pagamento único e antecipado	Pagamento antecipado em 5 parcelas fixas anuais	Economia com o pagamento único e antecipado
Tipo I	R$ 3.996.162,02	R$ 7.839.680,10	49,03%
Tipo III	R$ 2.740.770,49	R$ 4.455.967,70	38,5%

É importante ressaltar que este pagamento não se confunde com a antecipação de valores por serviços ainda não prestados. Trata-se da aquisição de um "Part Number" que assegura o direito à garantia estendida, atualizações e suporte para os equipamentos, diretamente com os fabricantes e em solidariedade com as contratadas. Não há, portanto, a contratação de uma prestação efetiva de serviços avulsos, mas sim a aquisição de um pacote que garante o direito a esses benefícios por um período determinado.

Considerando que as atualizações dos produtos são realizadas diretamente pelos fabricantes – empresas globalmente consolidadas no setor de equipamentos de firewall – o risco de futuras interrupções contratuais por falta de atendimento é extremamente baixo.

A liquidação e o pagamento serão assim efetuados:

a) os pagamentos serão realizados na forma do SIGEO JT - Sistema Integrado de Gestão Orçamentária e Financeira da Justiça do Trabalho - Módulo Execução Orçamentária.

b) para fins de liquidação e pagamento, é de exclusiva responsabilidade da Contratada o seu cadastramento no SIGEO, gestão de seus dados e a juntada por

meio do referido Sistema dos documentos de cobrança/documentos fiscais (notas fiscais/faturas);

c) é de exclusiva responsabilidade da Contratada as ações indicadas na alínea anterior não cabendo ao Contratante qualquer responsabilidade pela falta de juntada ao sistema no prazo;

d) eventuais dúvidas poderão ser dirimidas junto à Secretaria de Orçamento e Finanças por meio do email seof@trt12.jus.br ou telefone (48) 3216-4059.

e) a nota fiscal deverá ser juntada, pela Contratada no sistema SIGEO-JT Execução Financeira e os documentos exigidos no edital e no contrato deverão ser encaminhados ao Núcleo de Análise e Liquidação da Despesa – NULAD;

f) a equipe de gestão e fiscalização deverá proceder o recebimento provisório e definitivo do objeto, em conformidade com o art. 9º, da Portaria PRESI nº 775/2022;

g) o prazo para pagamento é de 10 (dez) dias úteis a contar da apresentação da fatura acompanhada do respectivo recebimento definitivo do objeto;

h) para todos os fins, considera-se como data de pagamento, o dia da emissão da ordem bancária;

i) havendo erro na(s) nota(s) fiscal(s)/fatura(s) ou qualquer circunstância que impeça a liquidação da despesa, aquela será restituída ou será comunicada a irregularidade à Contratada, interrompendo-se o prazo para pagamento até que esta providencie as medidas saneadoras.

j) os pagamentos serão realizados de acordo com o cronograma de desembolso do Governo Federal, em moeda corrente nacional, sendo retido na fonte os tributos e contribuições elencados na legislação vigente;

k) A Contratada será a responsável direta pelo faturamento a que se propõe, não podendo ser aceito documento de cobrança (nota fiscal/fatura) emitido por empresa com a raiz do Cadastro Nacional de Pessoa Jurídica – CNPJ diferente ao daquela, ainda que do mesmo grupo empresarial.

i. As Unidades responsáveis pela execução do objeto contratual e detentoras de numeração da raiz do CNPJ idêntica à da Contratada, divergindo somente o sufixo e dígito verificador, poderão emitir Nota Fiscal/Fatura, desde que satisfaçam as condições de habilitação e a regularidade fiscal exigida no processo;

l) a Contratada deverá apresentar, sempre que solicitado pelo Contratante, as certidões abaixo discriminadas:

i. CRF – Certificado de Regularidade do FGTS, emitido pela CEF;

ii. Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União, emitida em conjunto pela Secretaria da Receita Federal e Procuradoria-Geral da Fazenda Nacional.

iii. CNDT - Certidão Negativa de Débitos Trabalhistas, emitida pela Justiça do Trabalho;

iv. Prova de regularidade para com a Fazenda Estadual do seu domicílio ou de sua sede;

v. Prova de regularidade para com a Fazenda Municipal do seu domicílio ou de sua sede;

m) o Contratante poderá reter o pagamento dos valores referentes ao fornecimento realizado nas hipóteses da cláusula correspondente (cláusula que trata da responsabilidade civil), limitado ao valor do dano, ressalvada a possibilidade de rescisão contratual;

n) o Contratante poderá deduzir do montante a pagar, cautelar ou definitivamente, os valores correspondentes a multas ou indenizações devidas pela Contratada, nos termos deste contrato;

o) no ato do pagamento será retido na fonte o Imposto sobre a Renda de Pessoa Jurídica, a contribuição sobre o lucro, a contribuição para a seguridade social (CONFINS) e a contribuição para O PIS/PASEP, todos da Secretaria da Receita Federal. No entanto, não recairá esta retenção sobre pessoas jurídicas que apresentarem a Declaração de Optante do Simples, conforme modelo constante no Anexo IV da Instrução Normativa nº. 1.234/2012 , da Receita Federal ou cópia da Consulta ao Portal do Simples Nacional da apresentação da primeira nota fiscal/fatura decorrente de assinatura contratual e de prorrogação contratual;

p) se os valores do pagamento forem insuficientes para a quitação das eventuais multas, fica a Contratada obrigada a recolher a importância devida, via GRU, no prazo de até 10 (dez) dias contados da comunicação oficial, sob pena de ser incluído o valor na Dívida Ativa da União;

q) Nos casos de reajuste será utilizado o Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA. Será utilizado como marco para reajustamento a data do orçamento estimado, a saber: XX/XX/XXXX.

14. Penalidades

14.1. Para o Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento

O Tribunal utiliza como padrão as sanções descritas abaixo:

Pela inexecução total ou parcial do contrato, a Administração poderá, garantida a ampla defesa, aplicar à Contratada as seguintes sanções:

§ 1º – Em razão do descumprimento dos Níveis Mínimos de Serviço (Grupo IV - Serviço Gerenciado):

a) O descumprimento reiterado dos níveis mínimos de serviço resultará em punição indicada na Tabela TR12.

TR12 - Penalidades para os itens do Grupo IV

Quantidade de Descumprimentos Mensais			Penalidade
Severidade			
1 - Alta	2 - Média	3 - Baixa	
-	1	2	Advertência
1	2	3	Multa de 10%
2	3	4	Multa de 15%
Mais de 2	Mais de 3	Mais de 4	Multa de 20% e a equipe de fiscalização deverá avaliar a conveniência de proceder o distrato

b) Na hipótese de reincidência nos casos que prevêem a penalidade de advertência, em três meses seguidos ou em cinco alternados, a empresa será multada em 10% do valor mensal.

c) A indisponibilidade do registro de incidentes e do serviço de assistência técnica acarretará multa de 20% sobre o valor mensal e a equipe de fiscalização deverá avaliar a conveniência de proceder o distrato*;*

d) As multas previstas na tabela Tabela 10 - Penalidades para os itens do Grupo IV terão como base de cálculo o valor a ser pago à contratada mensalmente.

§ 2º – A Contratada ao cometer infrações nas licitações ou na execução contratual estará sujeita às seguintes penalidades:

I – Advertência, que será aplicada nas infrações contratuais leves, que não justifiquem a aplicação de penalidade mais rigorosa.

II – Multa, nos termos do inc. II do art. 156 da Lei 14.133/21, a ser aplicada a qualquer das infrações administrativas previstas no art. 155 da Lei 14.133/21:

a) multa moratória, pela infração administrativa prevista no inc. VII do art. 155 da Lei nº 14.133/21: decorrente de inobservância dos prazos para

cumprimento de obrigações contratuais, na forma definida no edital e no contrato, arbitrada em 0,3% (três décimos por cento) por dia sobre o valor do(s) item(s) em mora, limitada a 10%;

a.1) se o atraso for superior a 30 (trinta) dias, poderão ser aplicadas cumulativamente as penas de multa moratória e compensatória, facultando-se, ainda, promover a rescisão contratual;

a.2) não sendo possível quantificar o valor da multa moratória ou se ele mostrar-se incompatível com o disposto no art. 2º, parágrafo único, inciso VI, da Lei nº 9.784/99, a multa será de R$ 1.000,00, podendo este valor ser aplicado em dobro, se as circunstâncias do caso concreto assim recomendarem;

b) multa compensatória, a ser aplicada pelo cometimento de qualquer das infrações previstas no art. 155 da Lei nº 14.133/2021, na forma definida no edital, no contrato:

b.1) multa por inexecução parcial arbitrada em 10% (dez por cento) do item/valor mensal do contrato, e aplicada em dobro no caso de reincidência, por ocorrência das infrações administrativas previstas nos incisos I e II do art. 155 da Lei nº 14.133/21;

b.2) multa por inexecução total arbitrada em 10% (dez por cento) do valor total do contrato e aplicada por ocorrência da infração administrativa prevista no inc. III do art. 155 da Lei nº 14.133/21;

b.3) multa arbitrada em 10% (dez por cento) sobre o valor total do contrato, e aplicada em dobro no caso de reincidência, por ocorrência das infrações administrativas previstas nos inc. IV a XII do art. 155 da Lei nº 14.133/01;

b.4) multa de 1% (um por cento) sobre o valor da nota fiscal, a ser aplicada a cada ocorrência de violação da obrigação da manutenção da regularidade fiscal e trabalhista, durante toda a execução do contrato;

III – Impedimento de licitar e contratar com a União, nos termos do inc. III do art. 156 da Lei nº 14.133/21, pelo prazo máximo de até 3 (três) anos, que será aplicada por ocorrência das infrações administrativas previstas nos incisos II a VII do caput do art. 155 da Lei 14.133/21, quando não se justificar a imposição de penalidade mais grave;

IV – Declaração de inidoneidade para licitar ou contratar com a Administração Pública, nos termos do inc. IV do art. 156 da Lei nº 14.133/21, que será aplicada por ocorrência das infrações administrativas previstas nos incisos VIII a XII do caput do art. 155 da Lei nº 14.133/21, bem como pelas infrações administrativas previstas nos incisos II a VII do caput do referido artigo que justifiquem a imposição de penalidade mais grave que a sanção de impedimento, referida na alínea “c” deste parágrafo, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos;

V – As sanções previstas nos incisos I, III e IV, poderão ser aplicadas cumulativamente com a prevista no inciso II deste parágrafo.

§ 3º – Penalidades da Contratada em face da LGPD:

O descumprimento das obrigações relativas ao tratamento de dados previstas na cláusula correspondente incidirá nas seguintes penalidades:

a) até 10% (dez por cento) sobre o valor da contratação , na hipótese de utilização dos dados pessoais para finalidade diversa daquela estabelecida para a execução contratual;

b) até 20% (vinte por cento) sobre o valor da contratação , na hipótese de do compartilhamento não autorizado de dados pessoais com terceiros.

I – As penalidades previstas nas alíneas a e b serão aplicadas por ocorrência e , no caso de reincidência, serão aplicadas em dobro.

II – As penalidades previstas nas alíneas a e b não excluem a responsabilidade das empresas pela aplicação das sanções previstas no art. 52 e o ressarcimento de danos, na forma prevista no § 4º do art. 42, ambos da LGPD.

§ 4º – Na aplicação das penalidades previstas nesta cláusula, serão observados os conceitos, critérios, prazos e procedimentos estabelecidos na Portaria Presi nº 340/2022 do TRT da 12ª Região.

§ 5º Caso os prazos estabelecidos para garantia sejam extrapolados e não seja apresentada, ou não seja aceita justificativa para tal atraso, serão aplicadas multas conforme tabela abaixo:

Atraso na prestação da Garantia	1ª Ocorrência (% do valor do contrato)	Reincidência (1) (% do valor do contrato)
1 a 5 dias	1%	2%
6 a 10 dias	2%	4%
11 ou mais dias	3%	6%

(1) A reincidência fica configurada a partir do segundo atraso registrado no atendimento destes serviços, mesmo que tratem de equipamentos distintos.

§ 6º Para os itens 8 e 15, referentes aos treinamentos, o não fornecimento do certificado de conclusão, para os alunos que tiverem direito, no prazo de 10 dias após sua conclusão ensejará em multa de 5% por dia de atraso, tendo como referência o valor do respectivo voucher.

15. Informações complementares

Anderson Bastos
Telefone: (48) 3216-4125
E-mail: anderson.bastos@trt12.jus.br

16. Estimativa de custos[3]

[3] A Pesquisa de Preços deverá ser juntada ao PROAD em documento apartado conforme Portaria PRESI 339/2022.

Tabela EPPXXX - Preços Estimados para a contratação

Grupo 1 - Serviço de suporte e manutenção e expansão para solução de NG Firewall utilizada na JT					
Item	**Descrição**	**Qtde mín**	**Qtde máx**	**Valor Unitário**	**Valor Total**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**	**10**	**11**	**R$ 3.996.162,02**	**Mínimo R$ 30.961.620,20** **Máximo R$ 43.957.782,94**
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo II - Pagamento em parcela única, antecipada.**	**5**	**6**	**R$ 2.740.770,49**	**Mínimo R$ 13.703.852,45** **Máximo R$ 16.444.622,94**
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em parcela única, antecipada.**	**4**	**4**	**R$ 2.528.895,32**	**Mínimo R$ 10.115.581,28** **Máximo R$ 10.115.581,28**
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em 5 parcelas fixas anuais.**	**1**	**1**	**R$ 7.839.680,10 (1)**	**Mínimo R$ 7.839.680,10** **Máximo R$ 7.839.680,10**

5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em 5 parcelas fixas anuais.**	**1**	**1**	**R$ 4.455.967,70 (2)**	**Mínimo R$ 4.455.967,70** **Máximo R$ 4.455.967,70**
6	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo IV - Pagamento em parcela única, antecipada.**	**1**	**1**	**R$ 6.399.252,28**	**Mínimo R$ 6.399.252,28** **Máximo R$ 6.399.252,28**
7	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo V - Pagamento em parcela única, antecipada.**	**3**	**4**	**R$ 5.062.251,46**	**Mínimo R$ 15.186.754,38** **Máximo R$ 20.249.005,84**
8	Voucher de **Treinamento** para solução de proteção de perímetro de rede lógica do tipo Next Generation **Firewall**	**38**	**100**	**R$ 13.054,41**	**Mínimo R$ 496.067,58** **Máximo R$ 1.305.441,00**
Grupo 2 - Equipamento e licenças para conexão de SD-WAN via solução de Next Generation Firewall					
9	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls **Tipo I e Tipo IV**	**3**	**3**	**R$ 1.092.075,23**	**Mínimo R$ 3.276.225,69** **Máximo R$ 3.276.225,69**
10	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 2 e 7 - Firewalls **Tipo II e Tipo V**	**2**	**3**	**R$ 739.103,08**	**Mínimo R$ 1.478.206,00** **Máximo R$ 2.217.309,24**

11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VI**	**2**	**17**	**R$ 286.091,95**	**Mínimo R$ 572.183,90** **Máximo R$ 4.863.563,15**
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VII**	**18**	**68**	**R$ 266.887,93**	**Mínimo R$ 4.803.982,74** **Máximo R$ 18.148.379,24**
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VIII**	**4**	**64**	**R$ 193.879,44**	**Mínimo R$ 775.517,76** **Máximo R$ 12.408.284,16**
Grupo 3 -Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)					
14	Licença de uso de solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)** por usuário pelo período de 60 meses	**3700**	**28200**	**R$ 2.818,80(3)**	**Mínimo R$ 10.429.560,00** **Máximo R$ 79.490.160,00**
15	Voucher de Treinamento para solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)**	**33**	**120**	**R$ 12.836,38**	**Mínimo R$ 423.600,54** **Máximo R$ 1.540.365,60**
Grupo 4 - Serviço Gerenciado Mensal					
16	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) - **Tipo I e Tipo IV**	**9**	**10**	**R$ 894.864,60(3)**	**Mínimo R$ 8.053.781,40** **Máximo R$ 8.948.646,00**
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation	**6**	**8**	**R$ 894.864,60(3)**	**Mínimo R$ 5.369.187,60** **Máximo R$ 7.158.916,80**

	Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) - **Tipo II e Tipo V**				
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 5) - **Tipo III**	**4**	**4**	**R$ 894.864,60(3)**	**Mínimo R$ 3.579.458,40** **Máximo R$ 3.579.458,40**
19	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) - **Tipo VI, Tipo VII e Tipo VIII**	**18**	**81**	**R$ 54.528,00(3)**	**Mínimo R$ 981.504,00** **Máximo R$ 4.416.768,00**

(1) Valor total para 60 meses de contrato baseado em 5 parcelas fixas anuais de R$ 1.567.936,02.
(2) Valor total para 60 meses de contrato baseado em 5 parcelas fixas anuais de R$ 891.193,54.
(3) Valores unitários para 60 meses de contrato.

16.1 Estimativa de Custos para o TRT12

Item	Descrição	Unidade (1)	Valor unitário estimado	2025	2026	2027 e seguintes
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - Tipo II - Pagamento em parcela única, antecipada.	Cluster	R$ 2.740.770,49	R$ 2.740.770,49		
8	Voucher de Treinamento para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall	Aluno	R$ 13.054,41	R$ 78.326,46 (1)		
14	Licença de uso de solução de SASE (Secure Access Service	Usuário	R$ 563,76	R$ 28.188,00 (2)	R$ 112.752,00	R$ 112.752,00

	Edge) e ZTNA (Zero Trust Network Access) por usuário pelo período de 60 meses					
15	Voucher de Treinamento para solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access)	Aluno	R$ 12.836,38	R$ 77.018,28 (3)		
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) - Tipo II e Tipo V	Serviço/ Cluster	R$ 14.914,41	R$ 44.743,23 (4)	R$ 178.972,92	R$ 178.972,92
TOTAL				R$ 2.969.046,46	R$ 291.724,92	R$ 291.724,92

Para o TRT12 relativo ao ano de 2025:

(1) Foram previstas 6 unidades do Item 8.

(2) Foram calculados 3 meses para 200 usuários de SASE (Item 14) para o ano de 2025.

(3) Foram previstas 6 unidades do Item 15.

(4) Foram calculados 3 meses de serviço gerenciado (Item 17) para o ano de 2025.

17. Recursos orçamentários

No TRT 12 há previsão de recursos orçamentários para custear as despesas decorrentes da contratação ainda no presente exercício e a demanda está prevista no orçamento da Unidade Gestora.

Ptres: 168107

Programa de trabalho: 02.122.0033.4256.0042 - 0001 Manutenção e Gestão dos Serviços de Tecnologia da Informação

Itens	**Natureza da Despesa e Subelemento da Despesa**
1 a 5 - Suporte e Garantia Firewall	33904011 - Suporte de Infraestrutura de TIC

6, 7, 11, 12 e 13 - Aquisição Equipamentos Firewall	44905237 - Equipamentos de TIC - Ativos de Rede
8 e 15 - Treinamentos	33904020 - Treinamento/Capacitação em TIC
9 e 10 - Licenças SD-Wan	33904006 - Locação de Softwares
14 - Licença SASE/ZTNA	33904019 - Computação em Nuvem - Software como Serviço (SAAS)
16 a 19 - Serviço Gerenciado	33904011 - Suporte de Infraestrutura de TIC

18. Equipe de Planejamento da Contratação

Florianópolis, 18 de agosto de 2025

Integrante demandante:
Nome: Anderson Bastos
Matrícula: 2788
Lotação: Coordenadoria de Infraestrutura de TIC (INFRA)

Integrante demandante substituto:
Nome: Helton Alexander Michel
Matrícula: 3449
Lotação: Coordenadoria de Infraestrutura de TIC (INFRA)

Integrante técnico:
Nome: Paulo Seleme Corrêa
Matrícula: 4119
Lotação: Coordenadoria de Infraestrutura de TIC (INFRA)

Integrante técnico substituto:
Nome: George Alexandre Silva
Matrícula: 2490
Lotação: Coordenadoria de Infraestrutura de TIC (INFRA)

Integrante administrativo:
Nome: Alex Wagner Zolet

Matrícula: 4169

Lotação: Coordenadoria de Licitações e Contratos (CLC)

Integrante administrativo substituto:

Nome: Artur Prandin Cury

Matrícula: 4896

Lotação: Coordenadoria de Licitações e Contratos (CLC)

Anexo A - TERMO DE RECEBIMENTO PROVISÓRIO – Aquisições de bens

TERMO DE RECEBIMENTO PROVISÓRIO	
CONTRATO/PROAD Nº:	
UNIDADE:	
EMPRESA CONTRATADA:	
FISCAL DO CONTRATO:	
Nº DA NOTA DE EMPENHO:	
Nº DA NOTA FISCAL:	

1. **Do recebimento do material, verificar:**

Item	Descrição	Sim	Não	Não se Aplica
1.1	Se os materiais estão sendo entregues devidamente acondicionados em suas embalagens originais.			
1.2	Se as caixas em que se encontram os produtos estão em perfeitas condições de armazenamento.			
1.3	A data de validade dos materiais.			

2. **Da nota fiscal/fatura, em relação à Nota de Empenho e ao contrato, se houver, verificar se:**

Item	Descrição	Sim	Não	Não se Aplica
2.1	A razão social e CNPJ estão corretos.			
2.2	A data de emissão da nota fiscal/fatura é posterior à da Nota de Empenho.			
2.3	As descrições dos materiais estão corretas.			
2.4	O objeto corresponde aos critérios qualitativos e quantitativos estabelecidos no contrato/nota de empenho.			
2.5	A unidade, as quantidades e os valores unitário e total conferem com a respectiva Nota de Empenho e contrato (se houver) .			

3. **Outras observações pertinentes:**

Em[4] _____/_____/_____.

Ass.: _____
Fiscal Técnico do contrato
(informar nome)

[4] Atentar para a data do certifico do recebimento provisório, visto que servirá como base para a apuração de mora da empresa.

Anexo B - TERMO DE RECEBIMENTO PROVISÓRIO E DEFINITIVO – Serviços

CONTRATO/PROAD Nº:
UNIDADE:
EMPRESA CONTRATADA:
PERÍODO DE EXECUÇÃO DO SERVIÇO:
FISCAL DO CONTRATO:
Nº DA NOTA FISCAL[5]:

TERMO DE RECEBIMENTO PROVISÓRIO

Em cumprimento ao disposto no inciso I, alínea "a", do artigo 140, da Lei 14.133/2021, declaramos que:

( ) os serviços foram prestados neste Regional sem ressalvas.
( ) os serviços foram prestados neste Regional, com as seguintes ressalvas: Justifique e indique a cláusula contratual descumprida ou os indicadores dos Níveis Mínimos e Serviço correspondentes.

Em _____/_____/_____.

_____
Fiscal Técnico do contrato
(informar nome)

_____

TERMO DE RECEBIMENTO DEFINITIVO

Em cumprimento ao disposto no inciso III do §2º do art. 63 da Lei nº 4.320/64 declaro que o serviço descrito na (s) Nota (s) Fiscal (ais) acima indicada foi efetivamente prestado.

Existem ocorrências que interferem na liquidação e no pagamento da despesa?

( ) Sim. Justifique:
( ) Não.

[5] Se o recebimento for referente a mais de uma Nota Fiscal, devem ser indicados todos os documentos a que se refere.

Em _____/_____/_____.

Ass.: _____

Gestor(es) do contrato

Atentar para a segregação das funções de recebimentos provisório e definitivo

Anexo C - TERMO DE RECEBIMENTO DEFINITIVO - Aquisições de bens

TERMO DE RECEBIMENTO DEFINITIVO	
CONTRATO/PROAD Nº:	
UNIDADE:	
EMPRESA CONTRATADA:	
PERÍODO DE EXECUÇÃO DO SERVIÇO:	
FISCAL DO CONTRATO:	
Nº DA NOTA DE EMPENHO:	
Nº DA NOTA FISCAL:	

1. Do recebimento do material[6]:

Item	Descrição	Sim	Não	Não se Aplica
1.1	Verificar se os materiais estão em conformidade com a descrição na respectiva nota de empenho e contrato (se houver).			
1.2	Os testes realizados com os materiais e bens atendem ao solicitado/adquirido?			
1.3	Os materiais estão em perfeitas condições de uso?			

2. Da nota fiscal/fatura, em relação à Nota de Empenho e ao contrato, se houver:

Item	Descrição	Sim	Não	Não se Aplica
2.1	As descrições dos materiais estão corretas?			
2.2	A unidade, as quantidades e os valores unitário e total conferem com a respectiva nota de empenho e contrato (se houver)?			

3. Outras observações pertinentes:

Em[7] _____/_____/_____.

_____

(informar nome (s))

Gestor (es) do Contrato ou Comissão de Recebimento de Materiais de Consumo e/ou Permanente[8].

[6] Com exceção do subitem 1.2, todos os demais são de preenchimento obrigatório para o ateste definitivo para recebimento dos bens, cabendo à Equipe de Planejamento da Contratação, a cada caso concreto, incluir ou excluir itens levando em consideração as obrigações da contratada constantes do Termo de Referência.
[7] Atentar para a data do certifico do recebimento definitivo.
[8] Instituída no TRT12 pela Portaria PRESI nº 502/2021.

Atentar para a segregação das funções de recebimentos provisório e definitivo

Quando comissão, verificar se constam no mínimo 3 assinaturas.

Anexo D - Atestado de Conformidade para Pagamento da Nota Fiscal - Contratação de Serviços (continuados sem mão de obra residente, concessionárias de serviços públicos, locação de imóveis, serviços sob demanda e outros contratos)

LIQUIDAÇÃO DA NOTA FISCAL	
CONTRATO/PROAD Nº:	
UNIDADE:	
EMPRESA CONTRATADA:	
PERÍODO DE EXECUÇÃO DO SERVIÇO:	
RESPONSÁVEL:	

Item	SIM	NÃO	Não se aplica
1. NA LIQUIDAÇÃO MENSAL DA NOTA FISCAL:			
1.1 O Fiscal de Contrato atestou a conformidade na prestação dos serviços (Caso afirmativo informar o número do marcador do referido documento do respectivo PROAD)			
1.2 Valor da Nota Fiscal corresponde ao valor contratual mensal			
1.3 Verificar se o CNPJ da contratada contido na Nota Fiscal é o mesmo que consta da Nota de Empenho			
1.4 Período da prestação de serviços está correto (sempre corresponde ao mês anterior ao da fatura)			
2. VALIDADE DAS CERTIDÕES NEGATIVAS:			
2.1 Certidão Negativa de Débitos Trabalhistas			
2.2 GRF (FGTS)			
2.3 Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União			
2.4 Certidão Negativa de Débitos Salariais			
2.5 Prova de Regularidade com a Fazenda Estadual			
2.6 Prova de Regularidade com a Fazenda Municipal			

Em _____/_____/_____.

_____
Fiscal administrativo do contrato
(informar nome)

Anexo E - Atestado de Conformidade para Pagamento da Nota Fiscal - Aquisições de bens

LIQUIDAÇÃO DA NOTA FISCAL	
CONTRATO/PROAD Nº:	
UNIDADE:	
EMPRESA CONTRATADA:	
PERÍODO DE EXECUÇÃO DO SERVIÇO:	
RESPONSÁVEL:	

Item	SIM	NÃO	Não se aplica
1. NA LIQUIDAÇÃO MENSAL DA NOTA FISCAL:			
1.1 Houve recebimento provisório e definitivo da comissão de recebimento ou conforme especificado em contrato			
1.2 Valor da Nota Fiscal corresponde ao valor da nota de empenho			
1.3 Verificar se o CNPJ da contratada contido na Nota Fiscal é o mesmo que consta da Nota de Empenho			
1.4 Data de entrega da mercadoria de acordo com o edital ou contrato.			
2. VALIDADE DAS CERTIDÕES NEGATIVAS:			
2.1 Certidão negativa de débitos trabalhistas			
2.2 GRF (FGTS)			
2.3 Certidão conjunta de débitos relativos aos Tributos Federais e Dívida Ativa			
2.4 Prova de regularidade com a Fazenda Estadual			
2.5 Prova de regularidade com a Fazenda Municipal			

Em _____/_____/_____.

_____
Fiscal administrativo do contrato
(informar nome)

Anexo F - Termo de Encerramento de Contrato - Serviços (serviços sob demanda; serviços de prestação mensal e continuada (sem mão de obra residente); concessionárias de Serviço Público; locação de imóveis; outros contratos.

TERMO DE ENCERRAMENTO DE CONTRATO	
CONTRATO/PROAD Nº:	
UNIDADE:	
EMPRESA CONTRATADA:	
PERÍODO DA VIGÊNCIA DO CONTRATO:	
GESTOR DO CONTRATO:	

Item	SIM	NÃO	Não se aplica
1. A contratada atendeu e cumpriu as obrigações contratuais durante a sua vigência?			
2. Existe alguma pendência na prestação dos serviços, durante a vigência contratual? (Caso afirmativo relatar no item 6)			
3. Foi relatado ao gestor do contrato alguma pendência ou falta em que a contratada tenha incorrido durante a vigência do contrato? (Caso afirmativo relatar no item 6)			
4. Ocorreu alguma aplicação de penalidade à empresa contratada no período contratual? (Caso afirmativo relatar no item 6)			
5. Na avaliação de desempenho, caso previsto no contrato, a contratada atingiu os limites previstos? (Caso negativo relatar no item 6)			
6. Pendências contratuais:			
7. Outras observações:			
8. Atesto que não há pendências relativas à execução do objeto contratado. A empresa contratada prestou os serviços durante a vigência contratual em estrita observância às determinações, forma e condições previstas no contrato.			

Em _____/_____/_____.

_____
Gestor do contrato
(informar nome/carimbo)

Anexo G - Termo Final de Conformidade – Contratos de serviços continuados (sem mão-de-obra residente, concessionárias de serviços públicos, locação de imóveis e outros contratos continuados)

TERMO FINAL DE CONFORMIDADE	
CONTRATO/PROAD Nº:	
UNIDADE:	
EMPRESA CONTRATADA:	
PERÍODO DA VIGÊNCIA DO CONTRATO:	
RESPONSÁVEL:	

Item	SIM	NÃO	Não se aplica
1. Existe alguma pendência na validade das certidões negativas? (Caso afirmativo relatar no item 4)			
2. Existem pendências relativas à apresentação da documentação obrigatória da mão-de-obra diretamente envolvida na execução dos serviços? (Caso afirmativo relatar no item 4)			
3. Pendências de Certidões Negativas:			
4. Pendências relativas à documentação obrigatória da mão de obra envolvida:			
5. Atesto que não há pendências relativas à documentação das obrigações trabalhistas e demais obrigações referentes as condições de habilitação e qualificação exigidas, nos termos do inciso XVI, do art. 92, da Lei nº 14.133/2021			
6. Observações:			

Em _____/_____/_____.

_____
Fiscal administrativo do contrato
(informar nome/carimbo)

Anexo H - "Termo de Confidencialidade e de Responsabilidade"

Eu, (nome do profissional contratado), Inscrito no Cadastro de Pessoa Física(CPF) número (número do CPF do profissional), denominado PROFISSIONAL CONTRATADO da empresa (nome da empresa contratada),CNPJ (CNPJ da empresa contratada), denominada EMPREGADORA,declaro estar ciente das disposições abaixo, com as quais concordo plenamente.

O PROFISSIONAL CONTRATADO compromete-se a manter no mais absoluto sigilo e confidencialidade todas as informações do Tribunal Regional do Trabalho da 12ª Região, que, por qualquer meio, direta ou indiretamente,tomar conhecimento em razão dos serviços ora contratados.

O PROFISSIONAL CONTRATADO poderá ter acesso e conhecimento de informações e dados disponíveis do Tribunal Regional do Trabalho da 12ª Região, incluindo informações relativas aos servidores e magistrados,processos administrativos e judiciais, atividades de pesquisa, engenharia e desenvolvimento, tecnologia, pesquisa e métodos de processamento de dados, listas de usuários dos sistemas, dados sobre andamento processual,fornecedores, produtos, processos, listas de autores e réus em ações trabalhistas, informações financeiras, organizacionais, entre outros, devendo manter todas as informações em sigilo absoluto.

O PROFISSIONAL CONTRATADO tem ciência de que o tratamento dos dados a que poderá ter acesso, na forma como é descrito no art. 5º da Lei nº13.709/2018 – LGPD, será realizado exclusivamente nos limites e finalidades previstos no presente contrato. Declaro estar ciente de que, pela inobservância do acima exposto, poderei responder civil, penal e administrativamente, nos termos da lei.

MALOTE DIGITAL

Tipo de documento: Administrativo

Código de rastreabilidade: 512202525974320

Nome original: 4 - Anexo I - Especificações Técnicas da Solução de NGFW.pdf

Data: 19/08/2025 17:16:35

Remetente:

Tecnologia da Informação

Tecnologia da Informação

Tribunal Regional do Trabalho da 12ª Região

Documento: não assinado.

Prioridade: Normal.

Motivo de envio: Para conhecimento.

Assunto: Concordância dos órgãos participantes com os Estudos Técnicos Preliminares e Termo de Referência do registro de preços para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall.

Anexo I - Especificações Técnicas para Solução de Next Generation Firewall - NGFW

Inicialmente, apresenta-se na tabela A1 a lista de produtos previstos para aquisição como solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall

Tabela A1 - Produtos a serem adquiridos

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento		
Item	**Descrição**	**Unidade (1)**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**	Cluster
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo II - Pagamento em parcela única, antecipada.**	Cluster
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em parcela única, antecipada.**	Cluster
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em 5 parcelas fixas anuais.**	Cluster
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em 5 parcelas fixas anuais.**	Cluster
6	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo IV - Pagamento em parcela única, antecipada.**	Cluster

7	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo V - Pagamento em parcela única, antecipada.**	Cluster
8	Voucher de **Treinamento** para solução de proteção de perímetro de rede lógica do tipo Next Generation **Firewall**	Aluno
Grupo II - Aquisição de licenciamento e equipamentos para promover conexão de rede SD-WAN via Firewall		
9	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls **Tipo I e Tipo IV**	Licença/ Cluster
10	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 2 e 7 - Firewalls **Tipo II e Tipo V**	Licença/ Cluster
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VI**	Equip.
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VII**	Equip.
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VIII**	Equip.
Grupo III - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access) na modalidade Software como serviço e Treinamento		
14	Licença de uso de solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)** por usuário pelo período de 60 meses	Usuário
15	Voucher de Treinamento para solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)**	Aluno
Grupo IV - Serviço gerenciado mensal		
16	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) - **Tipo I e Tipo IV**	Serviço/ Cluster
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) - **Tipo II e Tipo V**	Serviço/ Cluster
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 5) - **Tipo III**	Serviço/ Cluster
19	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de	Serviço/ Equip.

	proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) - **Tipo VI, Tipo VII e Tipo VIII**	

(1) Ver definição de cluster abaixo.

Definições importantes:

Cluster: conjunto de dois, ou mais, equipamentos appliances compatíveis entre si, que trabalham de forma integrada e foram construídos especificamente para exercer a função de Next Generation Firewall.

Garantia de funcionamento: todos os serviços e atividades necessários para manter a solução em perfeito estado de funcionamento e que não envolvam operação ou configuração, tais como: manutenção corretiva, substituição de peças e componentes, substituição de equipamentos, atualizações de versões de *hardware* e *software*, revisões e/ou distribuições (*releases*) e correções (*patches*) dos programas (*softwares, firmwares, drivers*), etc. Deve incluir ainda o acesso, por meio da Internet, de base de documentos e conhecimentos mantida pela fabricante da solução, contemplando seus manuais de instalação. (responsabilidade do fabricante)

Atualização de assinaturas de proteção: acesso e meios para manter a solução em seu nível de identificação e proteção mais atualizado, tais como: atualização de assinaturas de prevenção de intrusão, assinaturas de identificação de vírus, assinaturas de identificação de aplicações, listas de classificação de URLs, listas de geolocalização, listas de endereços IPs utilizados por botnets, listas de endereços IPs de reputação duvidosa, etc. (responsabilidade do fabricante)

Suporte técnico: todos os serviços e atividades necessários à detecção de problemas de configuração e diagnóstico acerca de vícios e problemas dos produtos a fim de proporcionar o uso adequado e otimizado da solução, incluindo o esclarecimento de dúvidas,sugestão de melhores práticas e orientação técnica da Equipe Técnica do contratante.

A tabela A2 apresenta um compêndio dos prazos previstos na contratação.

Tabela A2 - Prazos da contratação

Item	Descrição da Atividade	Prazo
Itens 1, 2, 3, 4,e 5	Início do Serviço de garantia e atualização de assinaturas de proteção e suporte técnico	Até 10 dias após a comunicação da assinatura do contrato.
Itens 6 e 7	Entrega dos Equipamentos	Até 60 dias corridos contados da comunicação da assinatura do contrato.
	Reunião de Alinhamento Inicial	Em até 15 dias da comunicação da assinatura do contrato.
	Entrega do Plano de Trabalho (Cronograma e Escopo)	Em até 15 dias da reunião de alinhamento inicial.
	Análise do Plano de Trabalho	Em até 10 dias da entrega do Plano de Trabalho.
	Versão final do Plano de Trabalho	Em até 5 dias da resposta do TRT12 sobre a análise do Plano de Trabalho.
	Conclusão da Instalação	Até 90 dias da comunicação da assinatura do contrato.
	Início da Garantia e Suporte	Inicia com o recebimento definitivo do equipamento.
Item 8	Cursos disponíveis para as contratantes	Até 30 dias corridos após a comunicação da assinatura do contrato.
Itens 9 e 10	Fornecimento/Habilitação do serviço	Até 15 dias da solicitação da contratante.
Itens 11, 12 e 13	Entrega dos Equipamentos	De 1 a 20 equipamentos: Até 45 dias contados da comunicação da assinatura do contrato.
		Mais de 20 equipamentos: Até 90 dias contados da comunicação da assinatura do contrato.
	Reunião de Alinhamento Inicial	Em até 15 dias da comunicação da assinatura do contrato.
	Entrega do Plano de Trabalho (Cronograma e Escopo)	Em até 10 dias da reunião de alinhamento inicial.
	Análise do Plano de Trabalho	Em até 5 dias da entrega do Plano de Trabalho.
	Versão final do Plano de Trabalho	Em até 5 dias da resposta do TRT12 sobre a análise do Plano de Trabalho.
	Conclusão da Instalação	De 1 a 20 equipamentos: Até 60 dias da comunicação da assinatura do contrato.
		Mais de 20 equipamentos: Até 90 dias da

		comunicação da assinatura do contrato.
	Início da Garantia e Suporte	Inicia com o recebimento definitivo do equipamento.
Item 14	Disponível, para uso, integrada com a base de identificação de usuários do contratante	Até 60 dias da comunicação da assinatura do contrato.
Item 15	Cursos disponíveis para as contratantes	Até 30 dias corridos após a comunicação da assinatura do contrato.
Itens 16, 17, 18 e 19	Início do serviço	Equipamentos já instalados: Em até 15 dias da comunicação da assinatura do contrato.
		Equipamentos novos: com o recebimento definitivo dos equipamentos.

Antes de iniciar a descrição dos requisitos detalhados para a solução, como a solução de NG Firewall e SASE são complexos, implicam em risco de interrupção da prestação jurisdicional e ainda, em caso de substituição de fornecedor, é necessário obter nova quantidade profissionais terceiros e dos Tribunais para assegurar a continuidade da prestação, a EPC entende que, independente dos demais requisitos, o prazo de vigência de 60 meses é o mais adequado. Este período propiciará uma segurança para as equipes de TIC dos Tribunais, e também permitirá que as empresas amortizem seus investimentos em profissionais qualificados, garantindo maior concorrência, como também preços mais vantajosos considerando os custos de mobilização e desmobilização. Esse prazo também garante que a prestação jurisdicional não sofrerá pela troca de solução de Firewall, no mínimo, por 5 anos.

1. Requisitos para a Solução de NGFW - Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento

Esta seção trata de especificações para os equipamentos que compõem a Solução de alta disponibilidade de Next Generation Firewall, licenças e periféricos necessários para o seu pleno funcionamento nos ambientes *on premises* dos Órgãos públicos participantes.

Como o Firewall é uma solução que identifica e protege, em tempo real, Redes e dispositivos dos contratantes, que estão submetidos a ataques constantemente renovados, este mecanismo fica comprometido quando desatualizado. Portanto, é imprescindível assegurar que a solução de Firewall esteja sempre em sua versão mais recente.

O Grupo I foi definido em itens que englobam a renovação do serviço de garantia, atualização de assinaturas de proteção e suporte técnico para os equipamentos que já estão em uso nos tribunais participantes (itens de 1 a 5). Trata também da aquisição de novos equipamentos de NGFW vinculada a contratação conjunta do serviço de garantia, atualização de assinaturas de proteção (itens 6 e 7). O item 8 refere-se a aquisição de treinamento para capacitar os servidores que vão instalar, configurar e operar a solução.

1.1. Especificação dos Equipamentos do Grupo I itens 1 a 5 - dos Tipos I, II e III

Os equipamentos Tipos I, II e III são os equipamentos que foram dimensionados pelo fabricante Checkpoint para substituir os equipamentos que já estavam em operação nos tribunais que participaram da contratação de extensão de garantia Processos Administrativos 3928/2023 e 9665/2023 e que tiveram seus equipamentos antigos declarados como *end-of-life end-of-support* durante a vigência do contrato.

O Equipamento Tipo I é o modelo Quantum 16200 Plus do fabricante Checkpoint.

O Equipamento Tipo II corresponde aos modelos Quantum Force 9700/9800 Plus do fabricante Checkpoint.

O Equipamento Tipo III corresponde aos modelos Quantum 6700/9200 Plus do fabricante Checkpoint.

No caso de troca de equipamentos os novos equipamentos devem ter capacidade idêntica ou superior ao antigo e possibilitar o uso de todas as funcionalidades do equipamento anterior, bem como as especificações do item 1.4 deste Anexo.

O TRT12 ainda não fez a substituição do equipamento antigo 23500. Para este regional a contratação do Item 2 - Serviço de garantia e atualização de assinaturas de proteção e suporte técnico comporta também o fornecimento e

instalação do cluster de equipamentos 9800 Plus em sua capacidade máxima de memória e processamento.

1.2. Grupo I Item 6 do Edital - Aquisição de Cluster de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - Tipo IV - Pagamento em parcela única, antecipada.

Cada equipamento que compõe o cluster da solução Next Generation Firewall do Tipo IV deverá atender às seguintes especificações.

1.2.1. Throughput de NGFW mínimo esperado de, no mínimo, 45 Gbps (cinquenta Gigabits por segundo) e com, pelo menos, as funcionalidades de Firewall, IPS, Application Control e logs habilitadas;

1.2.2. Throughput de Threat Prevention de, no mínimo, 35 Gbps (trinta e cinco Gigabits por segundo) incluindo, pelo menos, as funcionalidades de Firewall, IPS, Application Control, filtro de URLs, proteção Anti-Malware e logs habilitados;

1.2.3. Número de conexões simultâneas de, no mínimo, 7.000.000 (sete milhões);

1.2.4. Número de novas conexões por segundo de, no mínimo, 350.000 (trezentos e cinquenta mil);

1.2.5. Deve suportar VPN IPSec *client-to-site* para no mínimo 6.000 usuários simultâneos;

1.2.6. Mínimo de 2 (dois) Discos Rígidos com capacidade, mínima, por disco de 480 GB (Gigabytes), tipo CFAST/SSD/M.2, operando em redundância, por appliance;

1.2.7. Mínimo de 4 (quatro) Interfaces QSFP28(100Gb)/QSFP+(40Gb) por appliance;

1.2.8. Mínimo de 16 (dezesseis) Interfaces SFP+(10Gb)/SFP(1Gb) por appliance;

1.2.9. Mínimo de 4 (quatro) portas 40Gb preenchidas com respectivo transceiver QSFP+, e adicionalmente, 16 (dezesseis) portas SFP+ 10Gb preenchidas com transceivers SFP+ 10GB-SR, para conexão via cabos de fibra óptica.

1.2.10. Devem ser fornecidos cordões ópticos de, no mínimo, 15m nas mesmas quantidades e compatíveis com os transceivers especificados no item anterior.

Observação: As taxas de transferência (*throughput*) e quantidades de conexões devem ser comprovadas por meio de documentação técnica oficial do fabricante da solução.

1.3. Grupo I Item 7 do Edital - Aquisição de Cluster de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - Tipo V - Pagamento em parcela única, antecipada.

Cada equipamento que compõe o cluster da solução Next Generation Firewall do Tipo V deverá atender às seguintes especificações.

1.3.1. Throughput de NGFW mínimo esperado de, no mínimo, 21 Gbps (vinte e um Gigabits por segundo) e com, pelo menos, as funcionalidades de Firewall, IPS, Application Control e logs habilitadas.

1.3.2. Throughput de Threat Prevention de, no mínimo, 20 Gbps (vinte Gigabits por segundo) incluindo, pelo menos, as funcionalidades de Firewall, IPS, Application Control, filtro de URLs, proteção Anti-Malware e logs habilitados.

1.3.3. Número de conexões simultâneas de, no mínimo, 3.000.000 (três milhões).

1.3.4. Número de novas conexões por segundo de, no mínimo, 240.000 (duzentos e quarenta mil).

1.3.5. Deve suportar VPN IPSec *client-to-site* para no mínimo 3.500 usuários simultâneos.

1.3.6. Mínimo de 2 (dois) Discos Rígidos com capacidade mínima, por disco, de 480 GB (Gigabytes), tipo CFAST/SSD/M.2, operando em redundância, por appliance.

1.3.7. Mínimo de 2 (duas) Interfaces QSFP28(100Gb)/QSFP+(40Gb) por appliance.

1.3.8. Mínimo de 8 (oito) Interfaces SFP+(10Gb)/SFP(1Gb) por appliance.

1.3.9. Mínimo de 4 (quatro) Interfaces UTP 1Gb (Gigabit), tipo RJ-45 por appliance.

1.3.10. Mínimo de 2 (duas) portas 40Gb preenchidas com respectivo transceiver QSFP+, e adicionalmente, 8 (oito) portas SFP+ 10Gb sendo 6 portas preenchidas com transceivers SFP+ 10GB-SR e duas portas preenchidas com 10GB-LR, para conexão via cabos de fibra óptica.

1.3.11. Devem ser fornecidos cordões ópticos de, no mínimo, 15m nas mesmas quantidades e compatíveis com os transceivers especificados no item anterior.

Observação: As taxas de transferência (throughput) e quantidades de conexões devem ser comprovadas por meio de documentação técnica oficial do fabricante da solução.

1.4. Características comuns para os equipamentos que compõem cada Cluster dos Itens 1 a 7 do Grupo I, Tipos I, II, III, IV e V

Os equipamentos que compõem os Clusters dos Itens 1 a 7, do Grupo I, da contratação, deverão ser do mesmo fabricante (Checkpoint), conforme justificativa constante no ETP.

O prazo de entrega é de 60 dias contados da comunicação da assinatura do contrato.

A seguir serão especificadas as características comuns para os equipamentos referentes ao Grupo I, itens 1 a 7[1] do Edital e Termo de Referência da presente contratação.

1.4.1. O *hardware* para cada equipamento appliance que compõem o cluster deve constar as seguintes características:

a) Deve ser apropriado para o uso em ambiente tropical, com umidade relativa entre 10 e 85% (sem condensação) e temperatura ambiente na faixa de 0°C a 40°C;
b) O fluxo do ar refrigerado deve ser recebido pela parte dianteira e dispensado na parte traseira do equipamento;
c) Possuir 2 (duas) fontes de alimentação independentes, redundantes e com capacidade de substituição sem desligar o equipamento (*hot-swappable*), com alimentação nominal de 100~120VAC e 210~230VAC, frequência de funcionamento de 50 ou 60Hz, ou ainda com ajuste automático de tensão e frequência (*auto-ranging*), por appliance;
d) Deverá vir acompanhado de cabos de alimentação para todas as fontes, com, no mínimo, 1,80m, com plugue tripolar 2P+T no padrão ABNT NBR 14136;
e) Deverá vir acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos, etc.) para fixação em bastidor (rack) padrão EIA-310 com largura de 19” (dezenove polegadas);
f) Possuir no mínimo 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI);
g) Possuir, no mínimo, 1 (uma) interface *out-of-band* dedicada para gerenciamento com capacidade compatível com o tipo do equipamento, I, II e III;
h) Possuir, no mínimo, 1 (uma) interface para o sincronismo de estados da solução de alta disponibilidade;

[1] As presentes especificações se aplicarão também caso os equipamentos que estejam abrangidos pelo serviço de suporte e garantia (Itens 1 a 7) precisem ser substituídos.

i) A interface de sincronismo não precisa, necessariamente, estar rotulada para a finalidade de sincronismo do recurso de alta disponibilidade, sendo aceitável qualquer interface do equipamento. A capacidade da interface deve ser compatível com cada tipo do equipamento, I, II e III;
j) Os equipamentos devem ser fornecidos em sua capacidade máxima de processamento e memória;
k) Possuir, no máximo, 4Us de altura;
l) Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, sem custos adicionais;
m) Possuir certificação de conformidade sustentável de acordo com os padrões EPA (Enviromental Protection Agency) ou similares, tais como EnergyStar, RoHS (Restriction on Hazardous Substances), WEEE (Waste Electrical and Electronic Equipment) ou EMI Certifications FCC part 15, CE, EN55022, EN55024;
n) Possuir certificação de conformidade da ANATEL ou serem fabricados no Brasil;
o) Deve informar, no painel de gerência do equipamento, a utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede, podendo ser mostrado também no sistema de gerência centralizado, e;
p) Deve informar, no painel de gerência do equipamento, o número de conexões simultâneas e de novas conexões por segundo do equipamento, podendo ser mostrado também no sistema de gerência centralizado.

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

1.4.3. Cada equipamento (appliance) deve oferecer, no mínimo, as seguintes funcionalidades:

a) Suportar os protocolos IPv4 e IPv6;
b) Suportar, no mínimo, 1.024 VLANs no padrão IEEE802.1q;
c) Suportar agregação de links no padrão IEEE802.3ad;
d) Suportar o protocolo DHCP;

e) Suportar o protocolo NTP;
f) Suportar as funcionalidades de roteamento estático e dinâmico, em IPv4 e IPv6;
g) Suportar os protocolos RIP, OSPF v2, OSPF v3, BGP v4 (RFC 4271) e BGP v6;
h) Suportar os protocolos IGMP v2, IGMP v3 e PIM-SM;
i) Suportar os protocolos SNMP v2c e SNMP v3;
j) Possuir Management Information Base (MIB) própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento;
k) Suportar Policy Based Routing (PBR), ou Policy Based Forwarding (PBF), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação;
l) Suportar o funcionamento nos modos sniffer (para inspeção de tráfego gerado por uma porta de rede espelhada), camada 2 de rede (*layer*-2), camada 3 de rede (*layer*-3), e suas combinações;
m) Permitir o acesso ao equipamento via CLI (console), SSH e interface web HTTPS;
n) Possuir funcionalidades de Backup/Restore de sua configuração e políticas de segurança;
o) Permitir o agendamento automático dos Backups, podendo ser realizado pela solução de gerenciamento;
p) Armazenar os Backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP e SCP, e;
q) Criptografar e autenticar a comunicação com a solução de gerenciamento centralizado.

1.4.4. Funcionalidades de identificação de usuários da solução (appliance):

a) Promover a integração com serviços de diretório LDAP, via serviço de diretórios OpenLDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos e ameaças;

b) Deve identificar de forma transparente os usuários autenticados por meio dos serviços de diretório OpenLDAP com protocolo LDAP, Microsoft Active Directory e servidores RADIUS, e ainda, para LDAP será admissível o uso de agentes nas estações de trabalho e servidores;
c) Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory, RADIUS e proxies internos;
d) Será permitido que a solução de gerenciamento centralizado possua um "appliance virtual" específico para atendimento às necessidades de identificação e autenticação de usuários;
e) Possuir portal de autenticação (*Captive Portal*) para a identificação e autenticação de usuários não registrados ou não reconhecidos por meio dos serviços de diretório OpenLDAP com protocolo LDAP, Microsoft Active Directory, servidores RADIUS;
f) O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP via serviço de diretórios OpenLDAP e Active Directory;
g) Permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP via serviço de diretórios OpenLDAP e Active Directory;
h) Registrar a identificação do usuário em todos os logs de eventos de acesso e de ameaças gerados pelo equipamento;
i) Registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (*batches*) ou processos de correlação após a ocorrência do evento em questão, e;
j) Deve estar licenciado e permitir a identificação e autenticação de pelo menos 10.000 (dez mil) usuários simultâneos.

1.4.5. Funcionalidades de Firewall por equipamento (appliance)

a) Não deve possuir restrições ao número de máquinas ou usuários protegidos;
b) Suportar a implementação tanto em modo transparente (*layer*-2) quanto em modo gateway (*layer*-3);
c) Suportar inspeção Stateful de tráfegos IPv4 e IPv6;

d) Suportar controle de acesso para pelo menos 90 serviços e protocolos pré-definidos;
e) Suportar os protocolos para transmissão de áudio e vídeo H.323, SIP e MGCP;
f) Suportar os protocolos de Streaming com compressão RTCP, RTMP, RTSP e RTP;
g) Implementar mecanismo de conversão de endereços NAT (*Network Address Translation*), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional (possibilitando que um endereço tenha mais de um NAT, dependendo da origem, destino ou porta);
h) Permitir transição entre endereços de redes IPv4 e IPv6, permitindo a comunicação entre dispositivos que usam esses protocolos diferentes, por meio de NAT N46 (que permite IPv4 acessar IPv6) e NAT64 (que permite IPv6 acessar IPv4).
i) Permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino;
j) Implementar mecanismo de proteção contra ataques de falsificação de endereços IP (*anti-spoofing*), tanto para IPv4 quanto para IPv6;
k) Implementar mecanismo de captura de pacotes;
l) Identificar os usuários para qualquer protocolo ou aplicação baseada em TCP/UDP, na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);
m) Suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6;
n) Suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período, e suas combinações;
o) Deve ser possível a aplicação de novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas, salvo as conexões atingidas pelas regras alteradas, e;
p) Possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando: Endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos de origem e destino, usuário identificado, status dos flags “ACK”, “SYN” e “FIN” ou sinalizar nos logs que o *Three-way-handshake* não foi concluído com sucesso, ação sobre o pacote (permitido ou negado).

q) A solução deve ser capaz de exportar dados de fluxo de tráfego (flows) para ferramentas externas de monitoramento e análise, usando protocolos tais como IPFIX (IP *Flow Information Export*) ou sFlow ou Netflow;

1.4.6. Funcionalidades de geolocalização por equipamento (*appliance*):

a) Identificar os países de origem e destino de todas as conexões estabelecidas com a Internet através do equipamento;
b) Suportar a atualização automática das listas de geolocalização;
c) Aplicar as atualizações sem perda das conexões ativas;
d) Armazenar as listas de geolocalização no próprio equipamento;
e) Permitir a criação de políticas de segurança baseadas em geolocalização, permitindo também o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países;
f) Possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças;

1.4.7. Funcionalidades de controle de acesso à Internet por equipamento (appliance)

a) Prover o controle e a proteção de acesso à Internet por meio do reconhecimento das aplicações, independente de porta e protocolo, e da classificação de URLs;
b) Identificar aplicações, independentemente das portas e protocolos, bem como das técnicas de evasão utilizadas;
c) Identificar se as aplicações estão utilizando sua porta default;
d) Identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS;
e) Identificar aplicações criptografadas usando SSL/TLS;
f) Identificar um mínimo de 5.000 (cinco mil) aplicações, incluindo, mas não se limitando a: *peer-to-peer*, *streaming* de áudio e vídeo, *update* de *software*, instant messaging, redes sociais, *proxies*, *anonymizers*, acesso e controle remoto, VoIP e e-mail;
g) Deve ser capaz de identificar, pelo menos, as seguintes aplicações: Torrent, TOR, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook,

Facebook Messenger ou Facebook Chat, Google+, Google Chat, Tinder, Instagram, Twitter (X), Linkedin, Dropbox, Google Drive, One Drive, Logmein, TeamViewer, MSRDP, VNC, Ultrasurf, Webex, Zoom;

h) Permitir a criação de assinaturas para identificação de aplicações proprietárias do órgão, sem a necessidade de ação ou intervenção do fabricante;
i) Suportar a atualização automática da base de assinaturas utilizada na identificação das aplicações;
j) Permitir aplicar as atualizações sem perda das conexões ativas e das assinaturas customizadas;
k) Armazenar preferencialmente a base de assinaturas no próprio equipamento, aceitando-se também na solução de gerenciamento centralizado;
l) Classificar as aplicações em categorias, tecnologia e fator de risco;
m) Identificar os usuários que estão utilizando as aplicações, na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);
n) Permitir o bloqueio de aplicações que não estejam utilizando suas portas default;
o) Suportar a implementação de políticas de segurança baseadas em: aplicações, categorias de aplicações, fator de risco, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo. As políticas descritas poderão ser aplicadas individualmente ou combinadas, conforme a necessidade da contratante;
p) Permitir a utilização ou bloqueio individualizado das aplicações, para determinados usuários ou grupo de usuários;
q) Permitir registrar todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado;
r) Permitir o controle de uso de banda de *download* ou *upload* utilizada pelas aplicações (*traffic shaping*) baseado em: endereço IP ou rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo. Os controles descritos poderão ser aplicados individualmente ou combinados, conforme a necessidade da contratante;
s) Deve ser capaz de efetuar a classificação de conteúdo de páginas web em HTTP e HTTPS, baseado em listas de categorias;

t) Possuir, no mínimo, 60 categorias de URLs, incluindo, mas não se limitando, às seguintes categorias ou suas semelhantes[2]: *adult, chat, drugs, gambling, games, hacking, hate speech, remote proxies, social networks, streaming média, violence, weapons*;

u) Permitir sobrescrever as categorias de uma URL que se considere indevidamente classificada;

v) Permitir a criação de categorias/listas customizadas;

w) Permitir a inclusão de URLs customizadas nas categorias já existentes ou previamente customizadas;

x) Suportar a atualização automática das listas de categorias, e aplicação das atualizações sem perda das conexões ativas e das URLs customizadas;

y) Armazenar as listas de categorias no próprio equipamento ou na solução de gerenciamento centralizado;

z) Deve identificar os usuários que estão acessando as páginas web na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);

aa) Suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, fator de risco, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo. As políticas descritas poderão ser implementadas individualmente ou combinados, conforme a necessidade da contratante;

bb) Alertar o usuário quando uma URL for bloqueada por meio da página de bloqueio que possa ser customizada no próprio equipamento, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada;

cc) Permitir o bloqueio e continuação da navegação web (possibilitando que o usuário acesse um site potencialmente bloqueado, informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão “Continuar” ou a inclusão de usuário e senha, para possibilitar o usuário continuar acessando o site), e;

dd) Registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado;

[2] O nome das categorias está em língua inglesa porque trata-se de uma prática comum entre os fabricantes de solução Firewall.

1.4.8. Funcionalidades de prevenção de ameaças por equipamento (appliance):

a) Possuir, no mínimo, funcionalidades de IPS, Antivírus, Anti-Bot, Anti-Malware e Anti-Spyware;
b) Possuir, no mínimo, os seguintes mecanismos de detecção: assinaturas de vulnerabilidades e exploits, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation, remontagem de pacotes TCP, detecção baseada em comportamento, nível de severidade do ataque e nível de confiança de detecção do ataque;
c) Possuir proteção contra ataques de negação de serviço DoS e DDoS;
d) Possuir assinaturas para bloqueio de ataques “buffer overflow”;
e) Possuir mecanismo automático de captura de pacotes de eventos de IPS, para fins de “troubleshooting” e análise forense;
f) Deve ser capaz de inspecionar tráfego criptografado usando protocolo SSL/TLS;
g) Deve ser capaz de inspecionar integralmente todos os pacotes de dados, sem prejuízo na performance do equipamento, para a seção 1.1 de acordo com os datasheets dos equipamentos já em operação e até os limites indicados nas seções 1.2 e 1.3;
h) Possuir referência cruzada da base de assinaturas de detecção com os identificadores CVE (*Common Vulnerabilities and Exposures*);
i) Possibilitar a criação de assinaturas customizadas;
j) Identificar os usuários relacionados aos eventos de IPS na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);
k) Possibilitar a criação de políticas de segurança que emitam alertas, sem realizar bloqueios, ao detectar a ocorrência de um ataque específico, identificando sua origem ou destino com base em um endereço IP ou rede CIDR específicos;
l) Permitir a criação de políticas de segurança capazes de bloquear ataques específicos por meio de ações como DROP (descarte) e/ou RESET (reinicialização da conexão), com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos;

m) Permitir a criação de exceções ou exclusões para a inspeção de uma determinada assinatura ou grupo de assinaturas, com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos;
n) Registrar todos os eventos de IPS, incluindo o usuário identificado;
o) Identificar e bloquear a comunicação com botnets;
p) Bloquear *malwares* e *spywares*;
q) Inspecionar e bloquear vírus, ao menos, nos seguintes tipos de tráfego: FTP, HTTP, HTTPS e SMTP;
r) Suportar proteção contra vírus em conteúdo HTML e javascript, *software* espião (*spyware*) e *worms*;
s) Suportar a inspeção de vírus em arquivos comprimidos utilizando algoritmo deflate, como o padrão zip, gzip, entre outros;
t) Suportar bloqueio de *download* de pelo menos 50 tipos de arquivos como, arquivos tipo Executáveis, PDF, DLLs, Arquivos de Código, MSI, doc, xls, ppt, entre outros;
u) Suportar a atualização automática das bases de assinaturas para prevenção de ameaças;
v) Suportar aplicação das atualizações de prevenção de ameaças sem reinicialização do equipamento e nem perda das conexões ativas que não sejam afetadas pelas atualizações;
w) Armazenar as bases de assinaturas de prevenção de ameaças no próprio equipamento ou na solução de gerenciamento centralizado;
x) Identificar os usuários relacionados aos eventos de bloqueio relacionados a prevenção de ameaças na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);
y) Permitir a criação de políticas de segurança que gerem alertas, sem realizar bloqueios, ao detectar a ocorrência de uma ameaça específica, com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos;
z) Permitir a criação de políticas de segurança que bloqueiem a ocorrência de ameaças específicas com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos, e;
aa) Suportar notificações e alertas sobre ameaças via e-mail, SNMP traps e log de pacotes;

1.4.9. Características de QoS por equipamento (*appliance*):

a) Permitir o controle de tráfego com base nas aplicações com, no mínimo as ações: permitir, negar, agendar o uso, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou cada usuário;
b) Suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp);
c) Suportar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP e RTP;
d) Suportar a marcação de pacotes DiffServ;
e) Permitir o monitoramento do uso da priorização de tráfego que as aplicações fazem por bytes, sessões e por usuário.

1.4.10. Características de inspeção SSL/TLS por equipamento (*appliance*):

a) Identificar, descriptografar e analisar o tráfego SSL e TLS 1.2/1.3 tanto em conexões de entrada (*Inbound*) quanto de saída (*Outbound*);
b) Deve permitir a descriptografia da área útil do pacote de dados (*payload*) para fins de controle de acesso à Internet e proteção contra ameaças, e;
c) Permitir a diferenciação de conexões pessoais (Bancos, *Shopping*, etc.) e conexões não pessoais por meio de classificação automática.

1.4.11. Características de VPN por equipamento (*appliance*):

a) Deve disponibilizar **licenciamento** para VPN *site-to-site*, sem limite do número de usuários simultâneos e sem limite do uso de túneis;
b) Suportar VPN *site-to-site* em topologias *Full Meshed* (todos os *gateways* possuem links específicos para todos os demais *gateways*) e também Estrela (*gateways* satélites se comunicam somente com um único *gateway* central);
c) Suportar, pelo menos, criptografias AES-128, AES-256;
d) Suportar integridade de dados com SHA-1 e SHA-256;
e) Suportar o protocolo IKE, fases I e II;

f) Suportar os algoritmos RSA e pelo menos 4 dos grupos Diffie-Hellman groups 1, 2, 5, 14, 15, 16, 17, 18;
g) Suportar NAT-T (NAT Transversal);
h) Deve possuir cliente próprio para instalação nos dispositivos fixos e móveis dos usuários, sem custo adicional e sem limite do número de usuários, e;
i) O cliente de VPN *client-to-site* deve ser compatível, ou suportar, o cliente nativo de pelo menos os seguintes Sistemas Operacionais: Windows 10 e Windows 11, Apple IOS versão 15 ou superior, Android versão 14 ou superior, Mac OS e Linux.
j) Deve permitir conexão VPN *client-to-site* de forma *Clientless*, com autenticação via *browser*, para fechar a VPN através de um portal TLS;
k) Deve suportar atribuição de endereço IP e de DNS dos clientes remotos de VPN;
l) Suportar Autenticação em Dois Fatores (2FA) para todos os usuários de VPN, sendo uma autenticação via usuário e senha, validados por bases LDAP com uso de serviço de diretórios OpenLdap, Active Directory, e base de usuários interna do appliance. Já o segundo fator pode ser Token gerado por e-mail (obrigatoriamente) e também protocolo TOTP e Certificado digital, admite-se ainda que o segundo fator seja implementado com ferramenta de terceiros;
m) Em relação ao certificado digital do item anterior, deverá ser compatível com: certificado emitido por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, CA externa de terceiros, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory, e certificados emitidos por autoridade certificadora no padrão ICP-Brasil;
n) O túnel VPN do cliente ao *gateway* (*client-to-site*) deve fornecer uma solução de autenticação única (*single-sign-on*) aos usuários, integrando-se, no mínimo, com as ferramentas de Windows *login* da empresa Microsoft;
o) Permitir criação de políticas para usuários e grupos para tráfego de VPN *client-to-site*;
p) Integrar com serviços diretórios LDAP, via OpenLDAP e Active Directory, para a autenticação de usuários de VPN e também definição de regras de acesso;
q) Permitir a definição de condições específicas para autorizar o acesso remoto às redes internas via VPN *client-to-site*, garantindo maior segurança e

controle. Entre essas condições, é necessário, no mínimo, suportar a verificação das versões dos Sistemas Operacionais dos dispositivos dos usuários, a exigência de um software antivírus instalado, ativo e com as definições atualizadas, e a validação das últimas atualizações "KBs" da Microsoft para ambientes Windows. Além disso, o sistema deve permitir a criação de uma lista de equipamentos autorizados, utilizando filtros como MAC-Address ou Hostname, e incluir restrições adicionais baseadas em registros do sistema (*registry*) do Windows. As condições descritas poderão ser aplicadas individualmente ou combinadas, conforme a necessidade da contratante;

r) Suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12[3];
s) Suportar a leitura e verificação de CRLs (*certification revogation lists*), e;
t) Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL/TLS.

1.4.12. Funcionalidades de Prevenção de Perda de Dados (*Data Loss Prevention*)

a) Evitar vazamento de informações em meio digital (*Data Loss Prevention* - DLP), atuando de maneira preventiva por meio do monitoramento de mensagens e arquivos transitados, e;
b) Caso seja identificado algum conteúdo que não deve ser transitado, a solução deve alertar o usuário que este conteúdo é sensível, ou mesmo bloquear o tráfego associado, baseado em filtros de conteúdo definidos pelo contratante.

1.4.13. Características da alta disponibilidade:

a) Deve operar em alta disponibilidade (HA) nativamente no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo, com sincronismo de estados integrado;

[3] O PKCS #12 faz parte da família de padrões chamados Public-Key Cryptography Standards (PKCS) publicados pela RSA Laboratories. Esse padrão de criptografia define um formato de arquivo para armazenar muitos objetos de criptografia como um único arquivo. E tal arquivo é usado para agrupar uma chave privada com seu certificado X.509 ou todos os membros de uma cadeia de confiança.

b) Suportar o balanceamento de carga interno na arquitetura ativo/ativo, disponibilizando a capacidade agregada dos dois equipamentos no cluster;
c) Suportar, no mínimo, 2 equipamentos por cluster. No caso de uso de três equipamentos será permitido que um permaneça em *stand by*;
d) Deve sincronizar entre os nós do Cluster todas as configurações recursos necessários para que a solução mantenha o funcionamento pleno em caso de falha de um dos equipamentos, como conexões e sessões TCP/IP, tabelas NAT, listas e assinaturas utilizadas para controle de acesso à Internet e proteção contra ameaças, tabelas FIB, associações de segurança das VPNs, entre outros.
e) Monitorar a falha dos links de comunicação e entre os nós do cluster;
f) Identificar e transferir automaticamente a operação do sistema (procedimento de *failover*) sempre que ocorrer: Falha de um cluster (quando existirem mais de um cluster instalado no contratante), transferindo a carga para o outro em data center distinto. Falha de um dos membros do cluster. Falha de qualquer componente ou processo crítico de um dos membros do cluster. Falha de um dos links de comunicação monitorados, e;
g) Deve ser capaz de realizar os procedimentos de failover sem perda das conexões ativas e interrupções no tráfego.

1.4.14. Funcionalidades para tratamento de ameaças desconhecidas (Zero-Day)

a) Deve contemplar ferramenta compatível com conceito de Sandboxing para prevenção de ataques *zero-day*;
b) Prevenção de ataques por meio do bloqueio efetivo de *malwares* desconhecidos (Dia Zero), oriundos da comunicação Web (HTTP e HTTPS), FTP, SMTP e IMAP/POP3 durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente;
c) O envio de conteúdo para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;
d) A funcionalidade de Sandbox deverá ser implementada em nuvem, appliance físico ou em ambiente virtual.

e) Caso a solução de Sandbox seja disponibilizada em ambiente virtual, é de responsabilidade da contratada providenciar servidores e softwares necessários para o funcionamento da ferramenta.
f) Deve ser capaz de enviar para análise, no mínimo, arquivos tipo Executável, PDF, DLLs, Arquivos de Código e MSI;
g) Suportar a análise de arquivos maliciosos em ambiente emulado e controlado com, no mínimo, os sistemas operacionais Windows 10 ou superior, Mac OS X ou superior;
h) Ser capaz de inspecionar e prevenir *malwares* desconhecidos em tráfego criptografado SSL/TLS;
i) Manter a performance sem degradação, independentemente das funcionalidades ativadas. (Ex.: AntiMalware, IPS, URL Filtering, e demais);
j) Geração de relatórios decorrentes das análises de links em Sandbox em caso de identificação de *malwares* e sites hospedeiros de exploits;
k) Deve ser capaz de classificar sites falsos, e atualizar a base do filtro URL da solução, e;
l) Deve prover análise em tempo real de páginas maliciosas e dessa forma, permitir o bloqueio de páginas maliciosas antes mesmo da atualização das bases de dados de URLs do fabricante da solução.

1.4.15. Administração e Gerência centralizada da solução de Next Generation Firewall.

1.4.15.1. A solução centralizada deverá gerenciar, de forma integrada, todos os equipamentos dos Grupos I e II que terão a renovação de garantia estendida ou que o órgão vier a adquirir, em qualquer combinação e quantidade dentro dos limites registrados.

1.4.15.2. A solução de gerenciamento centralizado deverá ser composta por, pelo menos, 1 (um) “appliance virtual” – solução de software baseada em máquina virtual, conforme os padrões estabelecidos pelo DMTF (*Distributed Management Task Force*), ou sistema operacional desenvolvido pelo próprio fabricante da solução de gerenciamento que possa ser instalado e executado em ambiente virtual.

1.4.15.3. Será instalada em ambiente de virtualização e *hardware* de propriedade do contratante.

1.4.15.4. A Licença de Software para administração / gerência deve estar disponível, para uso, integrada com a base de identificação de usuários do contratante, em até 60 dias da comunicação da assinatura do contrato.

1.4.15.5. A solução de gerência terá atualização e suporte pelo período de 60 meses a contar do seu recebimento definitivo. Deverá permitir sua utilização por tempo indeterminado, em sua última versão disponível na data do encerramento do período de 60 meses.

1.4.15.6. A solução de gerência deverá ser separada dos *gateways* de segurança, que irão gerenciar políticas de segurança de todos os *Firewalls* e funcionalidades solicitadas neste documento.

1.4.15.7. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução.

1.4.15.8. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos gerenciados via plataforma de segurança.

1.4.15.9. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento.

1.4.15.10. Suportar acesso via SSH para gerência, via cliente do próprio fabricante ou WEB (HTTPS).

1.4.15.11. O gerenciamento deve permitir/possuir monitoramento de logs, ferramentas de investigação de logs e acesso concorrente de administradores via contas diferentes.

1.4.15.12. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comando

1.4.15.13. A solução deve suportar a criação de regras com agendamento personalizado, permitindo configurar datas e horários de início e término para o uso de cada regra.

1.4.15.14. Suportar backup das configurações e reversão (*rollback)* de configuração, pelo menos, para a última configuração salva.

1.4.15.15. Suportar validação de regras antes da aplicação.

1.4.15.16. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras já existentes (*shadowing*).

1.4.15.17. Permitir a visualização dos logs em tempo real de uma regra específica, diretamente na mesma tela de configuração da regra selecionada, garantindo uma experiência integrada e facilitando o monitoramento e a análise imediata do tráfego associado.

1.4.15.18. Possibilitar a integração com, no mínimo, as soluções de SIEM IBM Qradar e Trend One, ferramentas que compõe a solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos que compõem a Ata de Registro de Preços n.20/2024, vigente, resultante do Pregão Eletrônico n.30/2024 - PROAD n. 22.093/2024 do TRT 2, contratada por vários órgãos participantes do presente processo.

1.4.15.19. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

1.4.15.20. Permitir a criação de certificados digitais para autenticação de usuários.

1.4.15.21. Geração de relatórios de todas as funcionalidades de segurança que estão ativadas nos GW's de segurança. Deve permitir apresentar eventos em um único portal (*dashboard*). Também devem existir relatórios e telas de apresentação onde sejam apresentados os principais eventos das funcionalidades de controle de

aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, *Anti-Malware* e *Sandboxing*).

1.4.15.22. Permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

1.4.15.23. Permitir a integração da ferramenta com provedores de identidade para autenticação dos administradores da solução via SAML 2.0.

1.4.15.24. Permitir que os administradores consigam revisar e aprovar alterações de políticas de segurança feitas por outros administradores.

1.4.15.25. Permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com no mínimo, os perfis de aprovador e solicitante.

1.4.15.26. Registrar logs, correlação de eventos e relatórios de auditoria dos administradores da solução.

1.4.15.27. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados.

1.4.15.28. Permitir a criação de relatórios personalizados.

1.4.15.29. Permitir criar relatórios com o resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais *hosts* por número de ameaças identificadas, atividades de usuários específicos e grupos de usuários do AD/LDAP. Os relatórios de usuários e grupos devem incluir as aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e *Anti-Malware*) de rede vinculadas a este tráfego.

Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, *Anti-Malware*), e URLs que passaram pela solução.

1.4.15.30. Possibilitar exportação dos logs em formatos CSV ou TXT.

1.4.15.31. Aplicar separadamente proteções relacionadas a ameaças e regras de acesso.

1.4.15.32. Para evitar erros na alteração de políticas, a solução deve combinar configuração de políticas e análise de logs em um único painel.

1.4.15.33. O visualizador de log deve ter um recurso de pesquisa.

1.4.15.34. Possibilitar a geração de relatórios de eventos no formato PDF ou HTML.

1.4.15.35. Possibilitar rotação do log.

1.4.15.36. O gerenciamento centralizado deverá ser entregue como appliance virtual em formato compatível/homologado com tecnologia VMWare ESXi.

1.4.15.37. A solução de gerenciamento deve possuir a capacidade de gerenciar outros Firewalls de segurança do mesmo fabricante mesmo estão em ambientes físicos (*on premises*), virtualizados e nuvens públicas (AWS e Azure) e nuvens privadas (VmWare NSX ou Cisco ACI).

1.4.15.38. Possuir capacidade de integração com soluções de terceiros via API e suportar configurações por meio de RestAPI.

1.4.15.39. Consolidar logs e relatórios de todos os dispositivos administrados pela gerência integrada.

1.4.15.40. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura.

1.4.15.41. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real.

1.4.15.42. Nas opções de Drill-Down deve ser possível identificar os acessos específicos de cada usuário.

1.4.15.43. Permitir que os relatórios possam ser salvos, enviados por e-mail e impressos.

1.4.15.44. Deve permitir a criação de filtros na visualização on-line dos relatórios com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.

1.4.15.45. Permitir visualização via painel de gerência on-line da quantidade de tráfego utilizado de aplicações e navegação para permitir análise avançada de incidentes.

1.4.15.46. Gerar relatório dos eventos de ataque de forma completamente visual, contendo, no mínimo, gráficos de consumo de banda utilizado pelos ataques e quantidade de eventos de segurança gerados e também eventos de segurança protegidos.

1.4.15.47. Permitir a integração com servidores de autenticação por meio dos serviços de diretório OpenLDAP com protocolo LDAP, Microsoft Active Directory e servidores RADIUS.

1.4.15.48. Criar certificados digitais para acesso dos usuários VPN.

1.4.15.49. Criar certificados digitais para VPNs *Site-to-Site*.

1.4.15.50. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplada a sua maior capacidade ou a capacidade de criação de certificados deve ser ilimitada.

1.4.15.51. Permitir criação de políticas de acesso de usuários autenticados por meio dos serviços de diretório OpenLDAP com protocolo LDAP e Microsoft Active Directory, de forma que os usuários sejam reconhecidos de forma transparente.

1.4.15.52. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças classificadas por origens e destinos do tráfego de dados.

1.4.15.53. Possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado, permitindo a procura correlacionada de logs em uma única tela, como por exemplo: pesquisar logs de Antivírus e navegação web simultaneamente na mesma consulta (*query* de pesquisa).

1.4.15.54. O relatório das emulações (*sandboxing*) deve conter deve conter um dos seguintes conjuntos de informações:

a) Print screen dos arquivos emulados, todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações individualizado para cada SO emulado, ou;
b) Tipo do arquivo, tamanho do arquivo, nome do arquivo, hash do arquivo, usuário que o recebeu, o veredito (um arquivo malicioso, um arquivo não malicioso e um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema).

1.4.15.55. Possibilitar a procura por IPs e redes, de forma que os resultados mostrem estes IPs e redes nos campos de origem e destino dos logs na mesma tela de pesquisa;

1.4.15.56. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

1.4.15.57. Capacidade de personalização de gráficos com os dados dos logs, como barra, linha e tabela;

1.4.15.58. Permitir a criação de painéis (*dashboards*) customizados para visualização do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

1.4.15.59. Possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema e dos componentes gerenciados por ele, contendo, no mínimo, licenças ativas, utilização de memória, utilização de discos e uso de CPUs;

1.4.15.60. Ser capaz de correlacionar eventos de todas as suas fontes de log em tempo real;

1.4.15.61. Fornecer conteúdo de correlação de eventos pré-definido organizado por categoria;

1.4.15.62. Monitorar alterações, análise e otimização de regras de políticas de segurança;

1.4.15.63. Possibilitar a verificação de regras de acesso por meio de uma consulta de origem, destino e serviço, a solução também deve apresentar se o tráfego está permitido, bloqueado ou parcialmente permitido/bloqueado, demonstrando os dispositivos no caminho, roteamento e interfaces;

1.4.15.64. Deve apresentar relatórios de otimização de regras e objetos, no mínimo, contendo as seguintes informações:

a) Regras não usadas;
b) Regras cobertas
c) Consolidar regras
d) Regras desabilitadas
e) Regras temporárias (definição de data e hora de funcionamento)
f) Regras mais usadas;

g) Última vez que uma regra foi usada;
h) Objetos duplicados;
i) Objetos vazios, e;
j) Serviços duplicados.

1.4.15.65. Permitir a monitoração de itens de configuração do sistema operacional dos dispositivos gerenciados;

1.4.15.66. Enviar alertas configuráveis sobre regras a expirar;

1.4.15.67. Emitir alertas em caso de alterações de configuração que não estão em conformidade com os padrões e políticas corporativas vigentes;

1.4.15.68. Realizar a comparação das configurações de um mesmo ou entre diferentes dispositivos;

1.4.15.69. Permitir o agendamento para a geração de relatórios dos dispositivos gerenciados;

1.4.15.70. Ser capaz de fornecer lista de usuários de VPN dos dispositivos gerenciados, no mínimo, baseados nos seguintes critérios:

a) Data de criação;
b) Grupos de usuários;
c) Métodos de autenticação dos usuários, e
d) Data de expiração dos usuários.

1.4.15.71. A comunicação entre a solução e os dispositivos de segurança gerenciados deve ser autenticada e criptografada;

1.4.15.72. Capacidade de comparar a base de regras do firewall com baselines padrão de mercado e fornecer um relatório de conformidade com o padrão utilizado na comparação;

1.4.15.73. Capacidade de migrar as regras e políticas dos dispositivos instalados nos contratantes para dispositivos substitutos, mesmo que de modelo e fabricante diferentes, utilizando a gerência ou ferramenta de terceiros.

1.4.15.74. Qualquer alteração na configuração dos dispositivos deve ser identificada automaticamente contendo as seguintes informações:

a) Qual foi a alteração;
b) Quem efetuou a alteração;
c) A data e hora da alteração;
d) Cada alteração nos dispositivos, deve ser identificado, no mínimo:
e) Alterações nas Regras (Criação, Remoção, Modificação);
f) Alteração nos Objetos de Redes e Serviços;
g) Alterações de Rotas ou Interfaces, e;
h) Visibilidade de toda alteração de configuração nos dispositivos.

1.4.15.75. O sistema deve realizar validação contínua das políticas e controles de segurança por meio de simulações em ambiente real; Deve possuir suporte de integração com plataformas de SIEM, permitindo análise e correlação de eventos em tempo real;

1.4.15.76. Possuir uma biblioteca de ameaças atualizada diariamente, contendo, no mínimo, 15.000 técnicas de táticas e procedimentos (TTPs) e 3.000 tipos de ameaças, incluindo *exploits* de vulnerabilidades e ataques APTs;

1.4.15.77. Possibilitar geração de relatórios personalizados que evidenciem mudanças na postura de segurança ao longo do tempo, incluindo recomendações específicas para mitigações baseadas no fornecedor e no cenário da ameaça;

1.4.15.78. Compatibilidade com ferramentas de segurança de rede, incluindo integração com plataformas de mercado para gestão de segurança;

1.14.16. Licenciamento das funcionalidades especificadas no Edital para os equipamentos (appliances)

Todas as funcionalidades descritas para a solução de Next Generation Firewall devem estar devidamente licenciadas e disponíveis para uso durante todo o período do contrato. Sendo elas, *Application Control*, identificação de usuários, *firewall*, geolocalização, navegação internet e inspeção de tráfego SSL/TLS, IPS, VPN, ameaças *zero-day, sandboxing, logging*, gerência centralizada, SD-WAN (caso contratada via Itens 10 e 11 deste Edital) e demais funcionalidades necessárias para completa utilização dos equipamentos.

1.14.17. Instalação do Cluster Grupo I itens 1 a 7

Os novos equipamentos adquiridos ou os equipamentos a serem substituídos por estarem em *end-of-support* deverão ser instalados seguindo o planejamento definido nesta subseção.

1.14.17.1. Requisitos Gerais da Instalação

1.14.17.1.1. Caberá à contratada todo o processo de planejamento, a instalação, a configuração, os testes, a migração e a compatibilidade dos equipamentos, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos equipamentos, como switchs, roteadores, equipamentos servidores, entre outros.

1.14.17.1.2. O processo de instalação, configuração, testes e migração deve acontecer em até 90 dias corridos após a comunicação da assinatura do contrato no caso de aquisição de novos equipamentos. Nos casos onde for decretado *end-of-support* para equipamentos dentro do prazo de vigência do contrato de garantia, o processo de instalação, configuração, testes e migração do equipamento a ser substituído deve ter como marco inicial a notificação da empresa sobre a necessidade de troca dos equipamentos.

1.14.17.1.3. A atividade de janela para efetiva entrada em produção do novo equipamento da solução de Firewall deverá ser agendada pelo contratante.

1.4.17.1.4. A contratada deverá realizar uma avaliação preliminar do ambiente de TI da contratante, incluindo uma análise da infraestrutura atual, para identificar quaisquer pré-requisitos ou necessidades de adaptação antes da implementação.

1.4.17.1.5. A Instalação terá quatro marcos: Reunião de Alinhamento Inicial; Entrega do Plano de Trabalho; Execução da instalação, migração e testes; Efetiva entrada em produção do novo equipamento.

1.4.17.1.6. 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.

1.4.17.1.7. A contratada deverá manter um canal de comunicação com a contratante durante a instalação/migração.

1.4.17.2. Requisitos de Instalação/migração

1.4.17.2.1. A instalação/migração não deve interromper as operações diárias da contratante sem agendamentos prévios e deve ser feita de forma a minimizar qualquer possível tempo de inatividade.

1.4.17.2.2. Eventuais necessidades de interrupção devem ser autorizadas e agendadas com a Administração do Órgão, com possibilidade de serem realizadas em finais de semana.

1.4.17.2.3. A instalação/migração envolverá as seguintes atividades:

a) Reunião de Alinhamento Inicial:
    i) A reunião de alinhamento inicial deverá ocorrer em até 15 dias da comunicação da assinatura do contrato.
    ii) Neste momento, a contratante deverá informar se a contratada deverá realizar a migração das configurações de solução de Firewall já instaladas, ou se prefere instalar uma configuração totalmente nova.

b) Entrega do Plano de Trabalho (Cronograma e Escopo):
   i) O Plano de Trabalho deverá contemplar ao menos: Declaração de Escopo, Matriz RACI, Cronograma (datas da Instalação Física e Lógica e Efetiva entrada em produção do novo equipamento), Recursos Humanos, procedimentos e testes a serem realizados no final da instalação
   ii) O documento em PDF deverá ser enviado para o Gestor e o Fiscal Técnico em até 15 dias da reunião de alinhamento inicial.
   iii) A contratante terá 10 dias para analisar o documento, realizando, por e-mail, as solicitações que entender cabíveis.
   iv) Sendo necessárias alterações a contratada terá 5 dias para apresentar, também por e-mail, a versão final.

c) Execução da instalação, migração e testes:
   i) Esta etapa terá início após a entrega dos equipamentos e deverá ser concluída em até 90 dias da comunicação da assinatura do contrato.
   ii) A contratada deverá disponibilizar o acompanhamento "on site" durante a instalação de, pelo menos, um especialista, certificado pelo fabricante do equipamento, para ser responsável pela execução da instalação, migração e testes, pelo tempo necessário, com, no mínimo, 40 horas de trabalho (sem contar a uma hora diária de almoço), sendo o limite de 9 horas diárias (incluindo uma hora para almoço), no horário das 8h às 17h;
   iii) Caso a instalação não seja concluída no período citado no item anterior, deverá haver um especialista técnico, em esquema de atendimento remoto, sendo o limite de 9 horas diárias (incluindo uma hora para almoço), no horário das 8h às 17h, que poderá ser acionado via telefone celular, até o recebimento definitivo do serviço de instalação.
   iv) A instalação física compreende a fixação, conexão de cabos de energia e lógicos de forma a possibilitar o funcionamento da solução de Cluster nas dependências do contratante
   v) Todas as conexões elétricas e lógicas utilizadas deverão ter seus cabos (rede, óticos e/ou elétricos) identificados (etiquetagem), sendo a

contratada responsável pelo fornecimento e impressão das etiquetas e materiais necessários para a organização, como presilhas, velcros, entre outros.

vi) A instalação lógica se inicia com a preparação dos equipamentos com 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.

vii) Quando solicitado pela contratante na reunião de alinhamento, a instalação compreenderá a migração das configurações e regras existentes no ambiente atual do contratante, suportado por um cluster de firewalls que pode ser de fabricante distinto da solução ofertada, assim como as demais configurações de segurança e disponibilidade.

viii) Transferência das configurações da solução atual para o novo equipamento, além de criação de novas regras e políticas que se mostrarem necessárias. 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;

ix) Validação dos dados criados nos novos equipamentos comparando-os com os dados dos equipamentos legados, garantindo a integridade das configurações;

x) Configuração lógica do equipamento para comunicação deste com a rede de dados da contratante.

xi) Realização dos testes especificados no item 1.4.17.2.4.

xii) Ao final da etapa de Execução da instalação, migração e testes, deverá ser enviado, para o e-mail do Gestor e do fiscal técnico, o Arquivo de configurações dos novos equipamentos.

d) Efetiva Entrada em Produção do Novo Equipamento:

i) Esta data deverá ser alinhada e autorizada pelo Gestor do contrato.

1.4.17.2.4. Testes

No intuito de validar o funcionamento das configurações realizadas, incluindo migração, devem ser realizados, no mínimo, os seguintes testes:

a) Deverá ser feito, no mínimo, dois tipos de acesso a partir da rede interna para a rede Servidores e para a rede DMZ.
   i) Acesso 1: utilizando protocolo https e sendo liberado o acesso, e;
   ii) Acesso 2: utilizando protocolo ssh e sendo bloqueado para a DMZ é liberado para a rede servidores;

b) Deverá ser feito um tipo de acesso externo com origem em um cliente VPN com destino a rede servidores.

c) Deverá ser exibido na console de gerência os registros que demonstrem:
   i) O horário da aplicação das últimas políticas;
   ii) A mudança realizada para bloqueio do Facebook;
   iii) O horário da mudança, e;
   iv) O administrador que realizou a mudança;

d) Deve ser desligada a PDU do nó ativo;
   i) Verificar se o nó passivo assumiu as operações com RTO[4]=0 (zero);
   ii) Ligar o appliance do nó ativo, e;
   iii) O nó ativo deverá assumir o controle das operações.

1.5. Características comuns para - Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - Grupo I Itens 1 a 7 (Equipamentos Tipo I, II, III, IV e V)

Entende-se apropriado apresentar um único conjunto de especificações para os serviços de garantia do Grupo itens 1 a 7, porque a única alteração entre estes itens é a capacidade do produto em que o serviço será aplicado.

[4] RTO (Recovery Time Objective) é a sigla em inglês para Objetivo de Tempo de Recuperação. É uma métrica que define o tempo máximo que um sistema pode ficar inativo após uma interrupção

Cada unidade do serviço atenderá um cluster de equipamentos.

Assim, para os Firewalls dos Tipos I, II e III (Itens 1 a 5) que terão a assinatura por 60 meses adicionais e os Tipos IV e V (itens 6 e 7) cuja contratação do serviço de garantia por 60 meses está vinculada a aquisição dos novos equipamentos, a contratada deve oferecer, no mínimo, os serviços de garantia e atualização conforme segue.

1.5.1. Os serviços de assistência técnica “on-site”, realizados pela contratada ou autorizados pela mesma mediante declaração expressa, deverão ser prestados nos municípios das sedes dos Tribunais, nas Capitais e suas respectivas regiões metropolitanas.

1.5.2. Todos os custos e encargos relacionados à execução dos serviços de garantia e assistência técnica necessários durante o prazo de garantia dos serviços e dos bens serão de responsabilidade integral da contratada.

1.5.3. A contratada deverá prestar serviço de manutenção e suporte técnico ao longo da vigência do contrato destinado a:

a) Restabelecimento de serviços interrompidos ou degradados;
b) Solução de problemas de configuração e falhas técnicas nos serviços;
c) Esclarecimentos de dúvidas sobre configurações e utilização dos serviços, e;
d) Implementação de novas funcionalidades.

1.5.4. A garantia e serviço de assistência técnica do produto ofertados deverão ser do Fabricante.

1.5.5. A assistência técnica da garantia consiste na reparação das eventuais falhas dos equipamentos, mediante a substituição de peças, componentes e acessórios que se apresentem defeituosos de acordo com os manuais e normas técnicas específicas para os equipamentos. No caso do modelo do equipamento haver sido descontinuado, um similar será aceito, desde que possua as características técnicas iguais ou superiores às exigidas no Edital.

1.5.6. O serviço de garantia deverá abranger os defeitos de hardware e de software, através de manutenção preventiva ou corretiva, incluindo a substituição de peças, partes, componentes e acessórios, sem representar quaisquer ônus para o Tribunal.

1.5.7. Os equipamentos devem contar com garantia de funcionamento, atualização de assinaturas de proteção e assistência técnica do fabricante, além do suporte técnico local e remoto pela Contratada, 24x7 (vinte e quatro horas por dia, sete dias na semana), pelo prazo de 60 (sessenta) meses.

1.5.8. Todas as partes e peças deverão ser substituídas pelos serviços de garantia, através de funcionários habilitados e credenciados para tal. Não serão aceitos o envio de peças/equipamentos pelos Correios, para que haja substituição por parte do Contratante. O Contratante não se responsabiliza por quaisquer danos aos equipamentos, que possam vir a ocorrer caso seja utilizada a prática de postagem pelos Correios.

1.5.9. Toda e qualquer substituição de peças e componentes deverá ser acompanhada por funcionário designado pelo Contratante, que autorizará a substituição das peças e componentes, os quais deverão ser novos e originais.

1.5.10. Em caso de necessidade de nova instalação e/ou configuração os serviços deverão ser realizados pela Contratada ou pelo Fabricante, por técnico certificado com capacidade técnica para a realização do serviço comprovada através da apresentação de documento de certificação emitido pela própria fabricante do equipamento ou por empresa de treinamento reconhecida pelo fabricante. Se necessário, a documentação original ou “as built” deverão ser atualizados pela contratada.

1.5.11. Os serviços de suporte que porventura implicarem na necessidade de desligamento de outros equipamentos, como servidores, storage, links, etc., deverão ser executados, preferencialmente, em horários fora do expediente, podendo inclusive ocorrer em finais de semana ou feriados, a critério do contratante.

1.5.12. A contratada deverá ter acesso completo aos Fóruns de Produtos do fabricante durante a vigência do contrato;

1.5.13. A contratada deverá ter acesso à base de conhecimento de suporte online do fabricante durante a vigência do contrato;

1.5.14. A contratada deverá ter cadastrado em portal do fabricante para *download* de *firmwares*, *patches* e *softwares* que fazem parte ou complementam a solução;

1.5.15. Serão aceitos modelo de suporte híbrido, em que os primeiros níveis são atendidos pela contratada e os últimos níveis pelo fabricante.

1.5.16. Níveis de Gravidade dos chamados para definição de tempos de atendimento.

1.5.16.1. Gravidade 1

a) Um erro com impacto direto na segurança do produto;
b) Um erro isolado no software ou dispositivo em um ambiente de produção que torna o produto inoperante; por exemplo, impacto crítico no sistema, queda do sistema;
c) Um defeito relatado no produto em um ambiente de produção, que não pode ser razoavelmente contornado, em que haja uma condição de emergência que restrinja significativamente o uso, como por exemplo, PJe fora do ar por problemas de configuração do sistema Firewall;
d) Produto para de executar as funções de negócios necessárias, como interrupção no acesso à Internet via rede Interna; ou
e) Incapacidade de usar o equipamento ou qualquer outro impacto crítico na operação do Firewall que exija uma solução imediata.

1.5.16.2. Gravidade 2

a) Um erro isolado no software ou no equipamento que degrade substancialmente o desempenho dos sistemas de TIC que dependem dele,

por exemplo, Sistema PJe acessível mas com performance muito degradada, lento e/ou com funcionalidades limitadas devido problemas de Firewall;

b) Um defeito que restringe o uso de um ou mais recursos mas não chega a afetar completamente o uso do Firewall, ou;
c) A utilização de uma função importante não está disponível e as operações são gravemente impactadas; por exemplo, lentidão nos sistemas da rede interna acessados via Internet.

1.5.16.3. Gravidade 3

a) Um erro isolado no Firewall que causa apenas um impacto moderado no uso do produto; por exemplo, Demora no login de sistemas via Internet, demora em algumas operações específicas do PJe, intermitência entre lentidão e desempenho satisfatório;
b) Um defeito que restringe o uso de um ou mais recursos do produto licenciado mas pode ser facilmente contornado, como parada do funcionamento da navegação Internet via rede Interna com autenticação de usuário e senha, mas que pode funcionar normalmente se liberada a autenticação até o problema ser resolvido, ou;
c) Um erro que pode causar algumas restrições funcionais, mas não tem um impacto crítico ou severo nas operações, como parada no acesso a sites de compra on-line.

1.5.16.4. Tempos de atendimento

Os tempos de atendimento estão descritos na tabela TR3, conforme segue.

Tabela A3 - Tempos de atendimento o Serviço de atualização de garantia

Serviço	**Tempo e condições**
Regime do atendimento	24x7
Tempo de resposta comprometido para problemas de Gravidade 1 (1)	30 minutos
Tempo de resposta comprometido para	Gravidade 2 - 2 horas

problemas de Gravidade 2 e 3 (1)	Gravidade 3 - 4 horas
Remessa de equipamentos em caso de necessidade de troca (RMA)	Próximo voo de saída/entrega expressa (quando aplicável) ou remessa no mesmo dia útil (2)

(1) Entende-se cumpridos os 30 minutos de tempo de atendimento caso haja comunicação em tempo real (chat, telefone). (2) Equipamentos são enviados durante o horário comercial normal e podem chegar fora do horário comercial.

1.5.17. A Contratada deverá providenciar o deslocamento de peças ou equipamentos para substituição bem como seu retorno sem qualquer ônus à contratante.

1.5.18. Todas as peças ou componentes utilizados/substituídos nos reparos deverão ser originais do fabricante, sem uso anterior e possuir, no mínimo, o mesmo desempenho e as mesmas garantias daqueles originalmente fornecidos.

1.5.19. Em caso de novos equipamentos, os mesmos devem ser compatíveis com os demais ativos de data center de cada Órgão participante. Ficará a cargo da contratada a verificação de compatibilidade antes da efetivação da reposição. Caso o sistema ofertado não tenha sua compatibilidade verificada, o correto funcionamento de todas as funcionalidades do sistema ofertado será de inteira responsabilidade da contratada, que deverá empreender todos os esforços necessários para entregar o sistema em pleno funcionamento, sob pena de arcar com as multas contratuais relativas a quebra de contrato.

1.5.20. Caso o equipamento não possa ser reparado dentro do prazo previsto, deverá ser providenciada pela contratada a instalação, em caráter provisório, de equipamento equivalente ou de configuração superior até que seja sanado o defeito do equipamento em reparo.

1.5.21. Caso os serviços de assistência técnica da garantia não possam ser executados nas dependências do contratante, o equipamento avariado poderá ser removido para o centro de atendimento da contratada. A contratada deverá fazer a justificativa por escrito relacionando os problemas apresentados que deverá ser apresentada ao setor competente do contratante que fará o aceite e providenciará a

autorização de saída do equipamento, desde que o mesmo seja substituído por outro equivalente ou de superior configuração, durante o período de reparo. O equipamento retirado para reparo deverá ser devolvido no prazo de 5 (cinco) dias úteis contados a partir da sua retirada.

1.5.22. A devolução de qualquer equipamento retirado para reparo deverá ser comunicada por escrito ao contratante.

1.5.23. A contratada deverá substituir o equipamento já instalado, por um novo e de primeiro uso, no prazo máximo de 2 (dois) dias corridos, na hipótese do mesmo equipamento apresentar defeito por 2 (duas) ou mais vezes dentro de um período de 20 (vinte) dias corridos.

1.5.24. Caso os equipamentos cobertos pelo serviço de garantia, atualização de assinaturas de proteção e suporte técnico vierem a ser declarados pelo fabricante em listas de *end-of-life*, *end-of-support* e/ou *end-of-sale* com essas datas terminando antes do período de vigência do contrato, os mesmos deverão ser substituídos pelos novos equipamentos indicados pelo fabricante em seu site, esses equipamentos devem ter capacidade idêntica ou superior ao equipamento antigo e possibilitar o uso de todas as funcionalidades do equipamento anterior.

1.5.25. Os serviços dependentes de atualização pela Internet e cujas licenças serão vinculadas à vigência do contrato, são: controle de acesso à Internet (controle de aplicações e filtragem de URLs), prevenção de ameaças (IPS, Antivírus, Anti-Bot, Anti-Malware, Anti-Spyware), prevenção de perda de dados (data loss prevention) e postura dos endpoints, e demais funcionalidades necessárias para completa utilização dos equipamentos.

1.5.26. O licenciamento deverá permitir a utilização da solução, por tempo indeterminado, em sua última versão disponível na data do encerramento dos serviços de garantia, suporte técnico e atualização de versões.

1.5.27. Vigência e início do contrato

Os serviços de garantia e atualização terão vigência de 60 meses com início a partir da emissão do termo de recebimento definitivo da ativação de licenças vinculadas aos equipamentos Firewall Tipos I, II e III, IV e V (Grupo I Itens 1 a 7 do Edital).

1.6. Grupo I item 8 - Voucher de Treinamento para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall

1.6.1. O Treinamento fornecerá uma compreensão dos conceitos básicos e das habilidades necessárias para configurar minimamente um sistema de Firewall.

1.6.2. O curso de nível básico, item 8 deste Edital, abrangerá configurações de políticas de Segurança, gerenciamento e monitoramento de uma rede segura, atualizações e configurações de um gateway de segurança e implementação de uma rede virtual privada.

1.6.3. O Treinamento deverá ser fornecido na forma de voucher[5] individual para treinamento oficial do fabricante;

1.6.4. A duração do treinamento deve ser de, no mínimo, 24 horas aula distribuídas em até 6 dias úteis, com um máximo de 8 horas aula por dia;

1.6.5. O treinamento e o material didático deverão ser em língua portuguesa;

1.6.6. O treinamento deverá ocorrer no período entre 8h00 e 18h00;

1.6.7. As turmas deverão ter até 15 alunos;

1.6.8. O treinamento deverá ser realizado de forma on-line e síncrona;

[5] Para o objeto definido nos itens 8 e 15 da presente contratação, o Voucher é um vale, ou valor em crédito, para realização de Treinamento Introdutório dentro de plataforma de educação à distância, que deve ser disponibilizado em turmas regulares dentro de um período específico de tempo, no caso, até 12 meses após a comunicação da assinatura do contrato.

1.6.9. Deverá ser fornecido certificado de conclusão do treinamento em até 10 dias após sua conclusão, contendo:

a) Nome do Aluno;
b) Nome do Curso;
c) Carga horária do Curso;
d) Data de início e fim do Curso;
e) Nome e assinatura do emissor, e;
f) Linguagem em Português do Brasil. Mesmos os certificados oficiais do fabricante.

1.6.10. As turmas para os cursos devem estar disponíveis para as contratantes em até 30 dias corridos após a comunicação da assinatura de cada contrato de aquisição de vouchers.

1.6.11. Devem haver turmas regulares até 12 meses depois da data da comunicação da assinatura de cada contrato.

1.6.12. A contratante deve ser comunicada mensalmente das turmas regulares e pode comunicar o uso do voucher do curso até, no mínimo, 15 dias antes do início da turma.

1.6.13. Conteúdo programático:

a) Introdução à tecnologia da Fabricante;
b) Gerenciamento de políticas de segurança;
c) Camadas de políticas;
d) Soluções e licenciamento da solução da fabricante;
e) Visibilidade do tráfego;
f) Conceitos básicos de VPN;
g) Gerenciando o acesso do usuário, e;
h) Implementação da tarefa do administrador.

2. Grupo II - Aquisição de licenciamento e equipamentos para promover conexão de rede SD-WAN via Firewall

Esta seção trata das especificações do Grupo II para aquisição dos equipamentos Next Generation Firewall (*appliance* SD-WAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - itens 11, 12 e 13 (Equipamentos Tipo VI, VII e VIII). Trata também dos itens 9 e 10 sobre licenciamento de Serviço de *Software-Defined* WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls Tipo I e Tipo IV e dos itens 2 e 7 Firewalls Tipo II, V para o seu pleno funcionamento nos ambientes *on premises* dos Órgãos públicos participantes.

Como mesmo em proporções menores, a Solução dos itens 11, 12 e 13 da contratação funcionam também como Firewall, que, como já dito, é uma solução que identifica e protege, em tempo real, Redes e dispositivos dos contratantes, que estão submetidos a ataques constantemente renovados, este mecanismo fica comprometido quando desatualizado. Portanto, é imprescindível assegurar que a solução de Firewall esteja sempre em sua versão mais recente. Por esse motivo a aquisição dos Itens 11, 12 e 13, também deverão estarão vinculadas ao serviço de garantia, atualização de assinaturas de proteção e suporte técnico.

2.1. Item 11 do Edital - Equipamento Next Generation Firewall (*appliance* SD-WAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - Tipo VI

O equipamento Next Generation Firewall do Tipo VI deverá atender às seguintes especificações:

2.1.1. Throughput de Threat Prevention de, no mínimo, 4 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente.

2.1.2. Suporte a, no mínimo, 600.000 (seiscentos mil) conexões simultâneas.

2.1.3. Suporte a, no mínimo, 28,000 (vinte e oito mil) conexões por segundo.

2.1.4. Throughput de, no mínimo, 2,4 Gbps para conexões VPN site-to-site.

2.1.5. Possuir, pelo menos, 8 (oito) interfaces de rede 1Gbps UTP;

2.1.6. Possuir, pelo menos, 2 (duas) interfaces de rede 1Gbps SFP;

2.1.7. Possuir, pelo menos, 2 (duas) interfaces de rede 1/10Gbps SFP+;

2.2. Item 12 do Edital - Equipamento Next Generation Firewall (*appliance* SD-WAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - Tipo VII

O equipamento Next Generation Firewall do Tipo VII - deverá atender às seguintes especificações:

2.2.1. Throughput de Threat Prevention de, no mínimo, 2Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente.

2.2.2. Suporte a, no mínimo, 400.000 (quatrocentos mil) conexões simultâneas.

2.2.3. Suporte a, no mínimo, 22.000 (vinte e dois mil) conexões por segundo.

2.2.4. Throughput de, no mínimo, 1.4 Gbps para conexões VPN site-to-site.

2.2.5. Possuir, pelo menos, 8 (oito) interfaces de rede 1Gbps UTP.

2.2.6. Possuir, pelo menos, 2 (duas) interfaces de rede 1Gbps SFP.

2.3. Item 13 do Edital - Equipamento Next Generation Firewall (*appliance* SD-WAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - Tipo VIII

O equipamento Next Generation Firewall do Tipo VIII deverá atender às seguintes especificações:

2.3.1. Throughput de Threat Prevention de, no mínimo, 650 Mbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero), habilitados simultaneamente.

2.3.2. Suporte a, no mínimo, 200.000 (duzentos mil) conexões simultâneas.

2.3.3. Suporte a, no mínimo, 15.000 (quize mil) conexões por segundo.

2.3.4. Throughput de, no mínimo, 1,2 Gbps para conexões VPN site-to-site.

2.3.5. Possuir, pelo menos, 8 (oito) interfaces de rede 1Gbps UTP;

2.3.6. Possuir, pelo menos, 1 (uma) interfaces de rede 1Gbps SFP;

2.4. Características comuns para os Itens 11, 12 e 13 do Edital, Equipamentos de Next Generation Firewall - Tipos VI, VII e VIII

Os equipamentos dos grupos I e II deverão ser do mesmo fabricante dos equipamentos hoje em uso (Fabricante Checkpoint), conforme justificativa constante no ETP.

A seguir serão especificadas as características comuns para os equipamentos referentes aos itens 11 a 13 desta especificação técnica.

2.4.1. Acerca das especificações sobre Software-Defined WAN (SD-WAN), a solução

deverá atender, no mínimo, os seguintes requisitos:

a) A solução de SD-WAN deve ser parte da solução de segurança, com políticas comuns ao firewall principal, gerência e logs centralizados;
b) A solução deve permitir conexão entre as unidades e o TRT via túnel criptografado (VPN *site-to-site*), e;
c) A solução deve permitir ao usuário da unidade remoto acesso à Internet diretamente, sem passar pelo firewall principal (TRT), mas com as mesmas políticas de segurança, inspeção e filtro de conteúdo, de acordo com o seu perfil.

2.4.2. Características Gerais

2.4.2.1. Suportar autenticação para o serviço NTP.

2.4.2.2. Deve suportar os protocolos RIP, OSPF v2, OSPF v3 e BGP v4 (RFC 4271).

2.4.2.3. Deve ser possível habilitar a interface LAN para encaminhar pacotes broadcast.

2.4.2.4. DHCP Relay

2.4.2.5. Possibilidade de definir por quais origens de rede são permitidas as conexões do administrador.

2.4.2.6. Os firewalls bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3.

2.4.2.7. Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos.

2.4.2.8. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

2.4.2.9. A solução deve ser capaz de permitir ao usuário acesso à Internet via canal privado (VPN com site principal) ou diretamente (via link de Internet), de acordo com as políticas definidas por tipo de aplicação, com todas as inspeções, para serviços de, pelo menos, os seguintes provedores de serviço em nuvem: Microsoft Azure, Google Services, Amazon AWS, Zoom.

2.4.2.10. A solução deve suportar a configuração manual de novos serviços, monitorando continuamente, pelo menos, latência, jitter e perda de pacotes.

2.4.2.11. Deverá suportar, através de interfaces Ethernet, simultaneamente múltiplos acessos através de diferentes meios de transmissão, como MPLS, Internet Banda Larga, 5G/4G.

2.4.2.12. Deverá possibilitar o encaminhamento de tráfego para saídas de Internet distintas por aplicação, sejam elas locais ou remotas.

2.4.2.13. Deverá ser possível preservar as marcações de QoS no cabeçalho do pacote original para os pacotes transportados.

2.4.2.14. Deverá ser possível configurar o dispositivo SD-WAN em alta disponibilidade, com redundância de pelo menos dois dispositivos, trabalhando em modo ativo/standby.

2.4.2.15. A solução deverá ser composta de hardware e software licenciado, do mesmo fabricante.

2.4.2.16. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de *software* livre.

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

2.4.2.18. Todos os componentes devem ser próprios para montagem em rack “19” e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação,

cabos de alimentação, suportes, gavetas e braços, se necessário.

2.4.2.19. A solução deve ser capaz de exportar dados de fluxo de tráfego (*flows*) para ferramentas externas de monitoramento e análise, usando protocolos tais como IPFIX (IP *Flow Information Export*) ou sFlow;

2.4.2.20. Possuir certificação de conformidade da ANATEL ou serem fabricados no Brasil;

2.4.3. Funcionalidade de Prevenção de Ameaças

2.4.3.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

2.4.3.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

2.4.3.3. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS SQL TCP, IKE aggressive Exchange;

2.4.3.4. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing);

2.4.3.5. Em cada proteção de segurança, devem estar incluídas informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;

2.4.3.6. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas

e customizadas;

2.4.3.7. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por, pelo menos. tipo de proteção, origem, destino, serviço e porta;

2.4.3.8. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

2.4.3.9. A funcionalidade de IPS e anti-bot, deve possuir capacidade de correlacionar em seus logs a visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela solução aberta;

2.4.3.10. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes;

2.4.3.11. A solução deve incluir ferramenta própria para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & control).

2.4.3.12. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

2.4.3.13. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

2.4.3.14. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

2.4.3.15. A solução de IPS deve suportar protocolos SMTP e POP 3, FTP, HTTP em qualquer porta.

2.4.3.16. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

a) Inspecionar tipos de arquivos conhecidos que contenham malware;
b) Inspecionar todos os tipos de arquivos, e;
c) Inspecionar tipos de arquivos de famílias específicas.

2.4.3.17. Deve bloquear acesso a URLs com malware.

2.4.3.18. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado.

2.4.4. Proteção Contra Ameaças Avançadas - *Zero Day*.

2.4.4.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT.

2.4.4.2. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo de comunicação Web (HTTP e HTTPS), FTP e E-mail (SMTP/TLS) via análise completa do arquivo no ambiente *sandbox*.

2.4.4.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL/TLS.

2.4.4.4. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas.

2.4.4.5. O conteúdo enviado para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado.

2.4.4.6. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, semanal e mensal, assim como o período de cada atualização.

2.4.4.7. Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing virtualizado ou em nuvem. Não serão aceitas soluções em servidores ou software livre.

2.4.4.8. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança.

2.4.4.9. Toda análise poderá ser realizada na nuvem do próprio fabricante, sendo aceitas soluções que necessitem de módulos e/ou servidores externos para a implementação de máquinas virtuais, desde que não seja solução de software livre.

2.4.4.10. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL/TLS.

2.4.4.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP.

2.4.4.12. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, outras extensões do pacote MS Office 365.

2.4.4.13. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

2.4.5. Filtro de Conteúdo Web

A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que

permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL.

2.4.5.1. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento.

2.4.5.2. Deve ser possível configurar o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como, ao menos, spyware, phishing, botnet, spam, tor, anonymizer, hacking ou categorias semelhantes.

2.4.5.3. Deve ser possível configurar o bloqueio a sites com conteúdo inapropriado como, ao menos, sexo, violência, armas, jogos e álcool.

2.4.5.4. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

a) Usuário ou grupo do Active Directory ou LDAP, e;
b) IP e/ou sub redes.

2.4.5.5. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como, por exemplo aplicações torrents e peer-to-peer.

2.4.5.6. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

2.4.5.7. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

2.4.5.8. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

a) Permitir especificar política por tempo, com definição de regras para um

determinado horário ou período (horário, diário, mensal e anual);

b) Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
c) Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório LDAP, via autenticação com tecnologia OpenLDAP, Active Directory e base de dados local;
d) Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
e) Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;
f) Bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;
g) Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;
h) Suportar a criação de categorias de URLs customizadas;
i) Permitir a customização de página de bloqueio, e;
j) Deve ser possível limitar o consumo de banda de aplicações.
k) Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

i - Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

ii - Reconhecer pelo menos 5.000 (cinco mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail, e;

iii - Deve ser possível realizar ou solicitar a recategorização de uma URL.

l) Deve descriptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3.

m) Para inspeção SSL/TLS, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE).

n) Para tráfego criptografado (SSL/TLS), deve decriptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

o) A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação.

p) Deve ser possível customizar a forma que serão exibidas as mensagens para os usuários nas seguintes ações:

i - Aceitar e informar;

ii - Bloquear e informar, e;

iii - Perguntar.

q) Deve ser totalmente compatível e integrada com a base de objetos e aplicações do Grupo I itens 1 a 7 (Solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) - Tipo I, Tipo II, TIpo III, Tipo IV e V), permitindo o uso de políticas semelhantes em todos os equipamentos, para que as unidades descentralizadas compartilhem com as diretrizes de navegação das Sedes.

2.4.6. Identificação de Usuários

2.4.6.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging;

2.4.6.2. Toda a solução proposta deverá ser implementada com autenticação dos usuários integrada e suportar aplicações de políticas granulares com base em nome do usuário, departamento e grupos, integrados com a plataforma Microsoft AD utilizando protocolo SAML (Security Assertion Markup Language) LDAP, Radius ou base de dados local;

2.4.6.3. A solução deve identificar usuários das seguintes fontes:

a) Active Directory - o *gateway* de segurança deve realizar consulta aos servidores AD para obter informação dos usuários, e;
b) Autenticação via navegador - Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador.
c) Para LDAP é admissível o uso de agentes nas estações de trabalho e servidores

2.4.6.4. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

2.4.6.5. Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scripts de comando;

2.4.6.6. Deve suportar o recebimento eventos de autenticação de soluções NAC via Radius ou API's ou Syslog, para a identificação de endereços IP e usuários;

2.4.7. Funcionalidade de VPN Site-to-Site

2.4.7.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;

2.4.7.2. A solução deve suportar autenticação com senha ou certificado;

2.4.7.3. Deverá permitir a comunicação híbrida através de localidades que se comunicam diretamente utilizando a topologia "mesh", e outras em que se faz necessária a centralização do tráfego utilizando uma topologia "hub-and-spoke";

2.4.7.4. Deverá estabelecer túneis dinâmicos, entre spokes estritamente mediante interesse de tráfego (rotas aprendidas) e para a totalidade de localidades spokes;

2.4.7.5. No caso da topologia "*hub-and-spoke*", deverá suportar mais de um ponto de concentração;

2.4.7.6. Deverá implementar de forma automatizada a constituição de túneis por meio da associação de perfis de configuração utilizando uma única interface gráfica;

2.4.7.7. A solução não deverá requerer configuração manual de endereçamento IP para a formação de túneis;

2.4.7.8. Deve suportar, pelo menos, criptografia AES 128 e 256;

2.4.7.9. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

2.4.7.10. O dispositivo deverá suportar mecanismo de prevenção contra loop de roteamento entre camada overlay e underlay;

2.4.8. Funcionalidades do SD-WAN

2.4.8.1. Detecção de falha em links e redirecionamento automático do tráfego para links alternativos, baseado em, pelo menos, latência, jitter e perda de pacotes.

2.4.8.2. Monitoramento contínuo de parâmetros de latência, jitter e perda de pacotes.

2.4.8.3. Deve ser capaz de classificar os links nas seguintes categorias/tags:

a) Preferível: Utilizar um tipo link a não ser que outro com melhor performance esteja disponível;
b) Evitar: Utilizar o link somente o necessário, e;
c) Não utilizar o link;

2.4.8.4. Aplicação de políticas de roteamento com base em classificação de tráfego (DPI – Deep Packet Inspection ou análise de cabeçalhos), mapeamento de portas e domínios de destino.

2.4.8.5. Seleção de caminhos de acordo com características técnicas, evitando degradação da qualidade de serviço:

a) Parâmetros de qualidade: níveis aceitáveis de latência, jitter, perda, definida por SLA, e;
b) Métricas utilizadas: comparação dinâmica do estado atual do link com os demais links disponíveis, para múltiplos destinos.

2.4.8.6. Suporte a múltiplos tipos de conectividade WAN, incluindo MPLS, com links com IP dinâmico e links com IP Fixo.

2.4.8.7. Ajuste automático do encaminhamento de pacotes perante variações nas condições dos enlaces de comunicação, por métrica e aplicação.

2.4.8.8. No caso de falha de um enlace, todas as conexões existentes devem ser automaticamente transferidas (*statefully*) para o outro enlace que estiver ativo, sem a necessidade de intervenção do administrador;

2.4.8.9. Deve permitir acrescentar novos enlaces de comunicação ao firewall sem que haja a necessidade de alterar enlaces existentes;

2.4.8.10. Deve fornecer o recurso de balanceamento de carga e agregação da capacidade de banda de enlace para estabelecimento de túneis VPN somando a capacidades destes enlaces de comunicação para o tráfego de dados dentro da VPN. Os enlaces devem ser agregados de modo a somar as capacidades dos enlaces;

2.4.8.11. Deve possuir funcionalidades de agregação de VPN *site-to-site*, baseando-se em políticas de VPN (quando a política define se o tráfego deve ser

enviado via (VPN) ou com base em rotas, suportando topologias em hub e spoke ou full-mesh.

2.4.8.12. Deve ter a capacidade de realizar a seleção de links/agregação de links de forma dinâmica e automática;

2.4.8.13. A agregação de link deve possibilitar pelo menos dois modos:

a) Balanceamento de carga (*load sharing*): tráfego balanceado entre diferentes enlaces com base em medida de desempenho (tempo ao destino) ou banda relativa entre enlaces;
b) Deve ser possível a seleção de determinado link de comunicação em função da aplicação de rede sendo trafegada;
c) Deve realizar a seleção do link e estado de link (ativo/standby) em função de aplicação sendo usada na rede, e;
d) Deve ser possível decidir por qual link outbound o tráfego será encaminhado em função da aplicação transportada (aplicação identificada por meio de análise de conteúdo de pacote e não simplesmente por meio de análise de portas UDP/TCP).

2.4.8.14. Os equipamentos devem possuir mecanismos para facilitar a instalação onde seja possível carregar a configuração remotamente de um escritório central ou da nuvem, restringindo a necessidade de interação local para localidades remotas.

2.4.8.15. Deverá suportar convergência rápida de tráfego de um túnel ao outro, sem perda de sessões TCP ou UDP previamente estabelecidas.

2.4.8.16. Deverá suportar a comutação de tráfego entre circuitos de dados.

2.4.8.17. A solução deverá implementar medição automática da qualidade dos circuitos.

2.4.8.18. A solução deverá se adaptar aos problemas de rede e mitigá-los sem intervenção humana.

2.4.9. Provisionamento de Serviço

2.4.10. A solução deverá suportar a ativação dos dispositivos SD-WAN por meio de tecnologia "*Zero Touch provisioning*", sem requerer configuração manual local no equipamento a ser ativado.

2.4.11. A solução deverá suportar a ativação "*Zero Touch provisioning*" dos dispositivos SD-WAN.

2.4.11.1. A ativação e o provisionamento "*Zero Touch provisioning*" deverão ser realizados sem a necessidade de configuração prévia do dispositivo SD-WAN;

2.4.11.2. O provisionamento de serviços deverá ser feito por meio da interface gráfica da Gerência centralizada, não sendo aceito provisionamento por meio de interface de linha de comando ou CLI (*Command Line Interface*);

2.4.11.3. As comunicações de provisionamento deverão ser protegidas e criptografadas;

2.4.11.4. O fluxo de trabalho de provisionamento não deverá requerer o uso de ferramentas externas, além das já incluídas, exceto DHCP;

2.4.11.5. As alterações de configuração deverão ser registradas e armazenadas para fins de auditoria.

2.4.12. Qualidade de Serviço (QoS)

2.4.12.1. Deverá ser capaz de aplicar QoS nos pacotes tratados pela solução, inclusive para tráfego de voz, vídeo, streaming, videoconferência e web conferência;

2.4.12.2. A solução deverá suportar QoS para proteção do tráfego das aplicações prioritárias do cliente em cenários de congestionamentos dos circuitos.

2.4.12.3. Poderá permitir métodos de priorização de tráfego baseado em classes ou critérios, suportando no mínimo 3 tipos (ou similares).

2.4.12.4. Poderá utilizar mecanismo de priorização do tipo Fair Queuing, buscando utilizar toda a banda útil disponível para as aplicações, respeitando a classe de tráfego.

2.4.12.5. Poderá ser possível criar políticas de QoS com algum dos seguintes recursos:

a) Remarcação de DSCP;
b) *Traffic Shapping*, e;
c) QoS Hierárquico ou similar.

2.4.12.6. A solução deverá suportar QoS nos túneis.

2.4.12.7. Desejável que a solução permita integração com políticas de QoS DiffServ existentes na rede MPLS;

2.4.12.8. A solução deverá permitir limitar uso de banda por interface e aplicação;

2.4.12.9. A aplicação de QoS deverá ser customizável, possibilitando uma solução flexível, que reconhece a aplicação e aplica uma marcação de prioridade. Com base nessa marcação de prioridade encaminha o tráfego pela WAN mais adequada e, para algumas aplicações mais críticas, enviando o pacote por mais de um caminho;

2.4.12.10. Deverá permitir classificação e/ou direcionamento do tráfego utilizando no mínimo 6 (seis) dos seguintes parâmetros:

a) Endereços e/ou faixa de endereços IP (rede e/ou subrede);
b) Classes de serviço;
c) Aplicação que utilize DPI (Deep Packet Inspection);
d) Fully Qualified Domain Name (FQDN) ou classificação baseada em nome de domínio;

e) Porta TCP/UDP – Origem e Destino;
f) Internet Protocol v4 (IPv4) – Origem e Destino;
g) Differentiated Services Code Point (DSCP);
h) Uniform Resource Locator (URL) ou FQDN, e;
i) Aplicação de camada 7 (Microsoft 365, Microsoft Office, Microsoft Exchange, Microsoft Sharepoint, Microsoft Teams, etc.).

2.4.12.11. Os objetivos de qualidade de serviço (QoS) serão aplicados em cada Fluxo de Aplicação (*Aplication Flow*) por meio de políticas específicas configuradas no Orquestrador. Estas políticas deverão maximizar a experiência de navegação do usuário da rede e do serviço VPN, dentro dos limites impostos pela banda contratada, podendo atuar na priorização do tráfego.

2.4.12.12. Desejável permitir métodos de priorização de tráfego (QoS) por tipo de protocolo e por serviços da pilha TCP/IP, além de *Traffic Policing* e *Traffic Shaping*: *Priority Queuing* e *Generic Traffic Shaping* (GTS).

2.4.12.13. Desejável permitir que, mesmo com o link degradado, a solução trabalhe de forma inteligente, juntamente com seus protocolos, para que esta degradação seja praticamente imperceptível ao usuário final.

2.4.12.14. Usar probes artificiais baseadas em icmp, udp ou tcp para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no mínimo jitter, latência e perda de pacotes.

2.4.12.15. Se houver necessidade de saída para internet via ponto remoto, deve ser possível selecionar por tipo de aplicativo.

2.4.12.16. Deve permitir a comunicação indireta entre localidades por meio de uma topologia “*hub and spoke*”.

2.4.12.17. Deve balancear o tráfego de aplicativos em vários links simultaneamente.

2.4.12.18. Redistribuição do tráfego balanceado, de forma inteligente, entre os links utilizados, em caso de falhas nestes links, ou de acordo com as políticas de qualidade pré-definidas.

2.4.12.19. Habilitar a mesma interface WAN para enviar tráfego simultaneamente por meio de túneis IPSec SD-WAN e nativamente fora dos túneis via underlay.

2.4.12.20. Habilitar a criação de políticas de negócios para controlar o padrão de redirecionamento de tráfego e aplicar qualidade de serviço.

2.4.12.21. Desejável suportar políticas inteligentes usando configuração padrão de fábrica que executem redirecionamento automático e imposição de QoS de voz, vídeo e tráfego transacional

2.4.12.22. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando políticas por aplicativo

2.4.12.23. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto centralizado, utilizando políticas por aplicativo.

2.4.12.24. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local.

2.4.13. Instalação equipamentos Grupo II itens 11, 12 e 13.

2.4.13.1. Caberá à contratada todo o processo de planejamento, a instalação, a configuração, a integração, os testes e a compatibilidade dos equipamentos, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos equipamentos, como Switchs, roteadores, equipamentos servidores, entre outros.

2.4.13.2. Para compras de 1 até 20 equipamentos, a instalação deverá ocorrer em até 60 dias corridos após a comunicação da assinatura do contrato.

2.4.13.3. Para compras de mais de 20 equipamentos, a instalação deverá ocorrer em até 90 dias corridos após a comunicação da assinatura do contrato.

2.4.13.4. A contratada deverá disponibilizar o acompanhamento remoto durante a instalação de, pelo menos, um especialista, certificado pelo fabricante do equipamento, para ser responsável pela atividade de instalação, com, no mínimo, 40 horas de trabalho (sem contar a uma hora diária de almoço), sendo o limite de 9 horas diárias (incluindo uma hora para almoço), no horário das 8h às 17h;

2.4.13.5. Requisitos de Instalação

2.4.13.5.1. A instalação/migração não deve interromper as operações diárias da contratante sem agendamentos prévios e deve ser feita de forma a minimizar qualquer possível tempo de inatividade.

2.4.13.5.2. Eventuais necessidades de interrupção devem ser autorizadas e agendadas com a Administração do Órgão, com possibilidade de serem realizadas em finais de semana.

2.4.13.5.3. A instalação/migração envolverá as seguintes atividades:

a) Reunião de Alinhamento Inicial:

   i) A reunião de alinhamento inicial deverá ocorrer em até 15 dias da comunicação da assinatura do contrato.

b) Entrega do Plano de Trabalho (Cronograma e Escopo):

   i) O Plano de Trabalho deverá contemplar ao menos: Declaração de Escopo, Cronograma (datas da Instalação Física e Lógica e Efetiva entrada em produção dos novos equipamentos), Recursos Humanos, procedimentos e testes a serem realizados no final da instalação

   ii) O documento em PDF deverá ser enviado para o Gestor e o Fiscal Técnico em até 10 dias da reunião de alinhamento inicial.

   iii) A contratante terá 5 dias para analisar o documento, realizando, por

e-mail, as solicitações que entender cabíveis.

iv) Sendo necessárias alterações a contratada terá 5 dias para apresentar, também por e-mail, a versão final.

e) Execução da instalação e testes:

i) Esta etapa terá início após a entrega dos equipamentos e deverá ser concluída em até 60 dias da comunicação da assinatura do contrato para compras de 1 a 20 equipamentos.

Em até 90 dias da comunicação da assinatura do contrato para compras de 21 ou mais equipamentos.

ii) Fornecimento de todos os acessórios para as conexões elétricas e lógicas utilizadas, como cabos (rede, óticos e/ou elétricos) e materiais necessários para a sua fixação como parafusos, engates, trilhos, entre outros.

iii) Preparação remota dos equipamentos com 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.

iv) Configuração lógica do equipamento para comunicação deste com a rede de dados da contratante.

v) Realização dos testes especificados no item 2.4.12.5.7.

vi) Ao final da etapa de Execução da instalação e testes, deverá ser enviado, para o e-mail do Gestor e do fiscal técnico, o arquivo de configurações dos novos equipamentos.

2.4.13.5.4. Quando o contratante também adquirir Clusters descritos no Grupo I itens 6 e 7 ou tiver instalado os itens de 1 a 5 do Grupo I, caso a contratante deseje, a transferência das configurações dos Clusters cabíveis para os Firewalls do tipo VI, VII e VIII, deverá ser realizada pela contratada;

2.4.13.5.5. Na instalação dos equipamentos, a contratada também deverá fazer a criação de novas regras e políticas que se mostrarem necessárias para a contratante.

2.4.13.5.6. Preferencialmente, o processo deverá ocorrer em ambiente apartado do ambiente produtivo;

2.4.13.5.7. Testes

No intuito de validar o funcionamento das configurações realizadas, incluindo migração, devem ser realizados, no mínimo, os seguintes testes:

a) Deverá ser feito, no mínimo, dois tipos de acesso a partir da rede interna.
   i) Acesso 1: utilizando protocolo https e sendo liberado o acesso, e;
   ii) Acesso 2: utilizando protocolo ssh e sendo bloqueado para a DMZ é liberado para a rede servidores;
e) Deverá ser feito um tipo de acesso externo com origem em um cliente VPN com destino a rede servidores.
f) Deverá ser exibido na console de gerência os registros que demonstrem:
   i) O horário da aplicação das últimas políticas;
   ii) A mudança realizada para bloqueio do Facebook;
   iii) O horário da mudança, e;
   iv) O administrador que realizou a mudança;

2.5. Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, por equipamento itens 11, 12 e 13 (Tipo VI, Tipo VII e Tipo VIII)

Entende-se apropriado apresentar um único conjunto de especificações para os serviços de garantia referente aos equipamentos do tipo VI, VII e VIII, porque a única alteração entre estes dois itens é a capacidade do produto em que o serviço será aplicado.

Assim, para os Firewalls dos Tipos VI, VII e VIII (Itens 11 a 13) deve a contratada oferecer, no mínimo, os serviços de garantia e atualização conforme segue.

2.5.1. Os serviços de assistência técnica “on-site”, realizados pela contratada ou

autorizados pela mesma mediante declaração expressa nas seguintes situações:

a) Quando atendimento remoto, deverão ser prestados no lugar onde o equipamento estiver instalado, em qualquer município do Brasil.
b) Quando atendimento para troca de peças e equipamentos com necessidade de presença física do técnico da contratada, nas Capitais e suas respectivas regiões metropolitanas.

2.5.2. Todos os custos e encargos relacionados à execução dos serviços de garantia e assistência técnica necessários durante o prazo de garantia dos serviços e dos bens serão de responsabilidade integral da contratada.

2.5.3. A contratada deverá prestar serviço de manutenção e suporte técnico ao longo da vigência do contrato destinado a:

e) Restabelecimento de serviços interrompidos ou degradados;
f) Solução de problemas de configuração e falhas técnicas nos serviços;
g) Esclarecimentos de dúvidas sobre configurações e utilização dos serviços, e;
h) Implementação de novas funcionalidades.

2.5.4. A garantia e serviço de assistência técnica do produto ofertados deverão ser do Fabricante.

2.5.5. A assistência técnica da garantia consiste na reparação das eventuais falhas dos equipamentos, mediante a substituição de peças, componentes e acessórios que se apresentem defeituosos de acordo com os manuais e normas técnicas específicas para os equipamentos. No caso do modelo do equipamento haver sido descontinuado, um similar será aceito, desde que possua as características técnicas iguais ou superiores às exigidas no Edital.

2.5.6. O serviço de garantia deverá abranger os defeitos de hardware e de software, através de manutenção preventiva ou corretiva, incluindo a substituição de peças, partes, componentes e acessórios, sem representar quaisquer ônus para o Tribunal.

2.5.7. Os equipamentos devem contar com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local e remoto pelo fabricante, 24x7 (vinte e quatro horas por dia, sete dias na semana), pelo prazo de 60 (sessenta) meses, incluindo serviços de instalação e configuração, o qual poderá ser prestado pelo integrador (contratada) desde que possua pessoal qualificado e certificado pelo fabricante.

2.5.8. Todas as partes e peças deverão ser substituídas pelos serviços de garantia, através de funcionários habilitados e credenciados para tal. Não serão aceitos o envio de peças/equipamentos pelos Correios, para que haja substituição por parte do Contratante. O Contratante não se responsabiliza por quaisquer danos aos equipamentos, que possam vir a ocorrer caso seja utilizada a prática de postagem pelos Correios.

2.5.9. Toda e qualquer substituição de peças e componentes deverá ser acompanhada por funcionário designado pelo Contratante, que autorizará a substituição das peças e componentes, os quais deverão ser novos e originais.

2.5.10. Em caso de necessidade de nova instalação e/ou configuração os serviços deverão ser realizados pela Contratada ou pelo Fabricante, por técnico certificado com capacidade técnica para a realização do serviço comprovada através da apresentação de documento de certificação emitido pela própria fabricante do equipamento ou por empresa de treinamento reconhecida pelo fabricante. Se necessário, a documentação original ou “as built” deverão ser atualizados pela contratada.

2.5.11. Os serviços de suporte que porventura implicarem na necessidade de desligamento de outros equipamentos, como servidores, storage, links, etc., deverão ser executados, preferencialmente, em horários fora do expediente, podendo inclusive ocorrer em finais de semana ou feriados, a critério do contratante.

2.5.12. A contratada deverá ter acesso completo aos Fóruns de Produtos do fabricante durante a vigência do contrato;

2.5.13. A contratada deverá ter acesso à base de conhecimento de suporte online do fabricante durante a vigência do contrato;

2.5.14. A contratada deverá ter cadastrado em portal do fabricante para *download* de *firmwares*, *patches* e *softwares* que fazem parte ou complementam a solução;

2.5.15. Serão aceitos modelo de suporte híbrido, em que os primeiros níveis são atendidos pela contratada e os últimos níveis pelo fabricante.

2.5.16. Níveis de Gravidade dos chamados para definição de tempos de atendimento.

2.5.17.1. Gravidade 1

a) Um erro com impacto direto na segurança do produto;
b) Um erro isolado no software ou dispositivo em um ambiente de produção que torna o produto inoperante; por exemplo, impacto crítico no sistema, queda do sistema;
c) Um defeito relatado no produto em um ambiente de produção, que não pode ser razoavelmente contornado, em que haja uma condição de emergência que restrinja significativamente o uso, como por exemplo, PJe fora do ar por problemas de configuração do sistema Firewall;
d) Produto para de executar as funções de negócios necessárias, como interrupção no acesso à Internet via rede Interna; ou
e) Incapacidade de usar o equipamento ou qualquer outro impacto crítico na operação do Firewall que exija uma solução imediata.

2.5.17.2. Gravidade 2

a) Um erro isolado no software ou no equipamento que degrade substancialmente o desempenho dos sistemas de TIC que dependem dele, por exemplo, Sistema PJe acessível mas com performance muito degradada, lento e/ou com funcionalidades limitadas devido problemas de Firewall;

b) Um defeito que restringe o uso de um ou mais recursos mas não chega a afetar completamente o uso do Firewall, ou;
c) A utilização de uma função importante não está disponível e as operações são gravemente impactadas; por exemplo, lentidão nos sistemas da rede interna acessados via Internet.

2.5.17.3. Gravidade 3

a) Um erro isolado no Firewall que causa apenas um impacto moderado no uso do produto; por exemplo, Demora no login de sistemas via Internet, demora em algumas operações específicas do PJe, intermitência entre lentidão e desempenho satisfatório;
b) Um defeito que restringe o uso de um ou mais recursos do produto licenciado mas pode ser facilmente contornado, como parada do funcionamento da navegação Internet via rede Interna com autenticação de usuário e senha, mas que pode funcionar normalmente se liberada a autenticação até o problema ser resolvido, ou;
c) Um erro que pode causar algumas restrições funcionais, mas não tem um impacto crítico ou severo nas operações, como parada no acesso a sites de compra on-line.

2.5.17.4. Tempos de atendimento

Os tempos de atendimento estão descritos na tabela A4, conforme segue.

Tabela A4 - Tempos de atendimento o Serviço de atualização de garantia

Serviço	**Tempo e condições**
Regime do atendimento	24x7
Tempo de resposta comprometido para problemas de Gravidade 1 (1)	1hora e 30 minutos
Tempo de resposta comprometido para problemas de Gravidade 2 e 3 (1)	Gravidade 2 - 3 horas Gravidade 3 - 5 horas
Remessa de equipamentos em caso de necessidade de troca (RMA)	Próximo voo de saída/entrega expressa (quando aplicável) ou remessa no próximo

	dia útil (2)

(1) Entende-se cumprido o tempo de uma 1 hora e 30 minutos de tempo de atendimento caso haja comunicação em tempo real (chat, telefone). (2) Equipamentos são enviados durante o horário comercial normal e podem chegar fora do horário comercial.

2.5.18. A Contratada deverá providenciar o deslocamento de peças ou equipamentos para substituição bem como seu retorno sem qualquer ônus à contratante.

2.5.19. Todas as peças ou componentes utilizados/substituídos nos reparos deverão ser originais do fabricante, sem uso anterior e possuir, no mínimo, o mesmo desempenho e as mesmas garantias daqueles originalmente fornecidos.

2.5.20. Em caso de novos equipamentos, os mesmos devem ser compatíveis com os demais ativos de data center de cada Órgão participante. Ficará a cargo da contratada a verificação de compatibilidade antes da efetivação da reposição. Caso o sistema ofertado não tenha sua compatibilidade verificada, o correto funcionamento de todas as funcionalidades do sistema ofertado será de inteira responsabilidade da contratada, que deverá empreender todos os esforços necessários para entregar o sistema em pleno funcionamento, sob pena de arcar com as multas contratuais relativas a quebra de contrato.

2.5.21. Caso o equipamento não possa ser reparado dentro do prazo previsto, deverá ser providenciada pela contratada a instalação, em caráter provisório, de equipamento equivalente ou de configuração superior até que seja sanado o defeito do equipamento em reparo.

2.5.22. Caso os serviços de assistência técnica da garantia não possam ser executados nas dependências do contratante, o equipamento avariado poderá ser removido para o centro de atendimento da contratada. A contratada deverá fazer a justificativa por escrito relacionando os problemas apresentados que deverá ser apresentada ao setor competente do contratante que fará o aceite e providenciará a autorização de saída do equipamento, desde que o mesmo seja substituído por outro equivalente ou de superior configuração, durante o período de reparo. O

equipamento retirado para reparo deverá ser devolvido no prazo de 5 (cinco) dias úteis contados a partir da sua retirada.

2.5.23. A devolução de qualquer equipamento retirado para reparo deverá ser comunicada por escrito ao contratante.

2.5.24. A contratada deverá substituir o equipamento já instalado, por um novo e de primeiro uso, no prazo máximo de 2 (dois) dias corridos, na hipótese do mesmo equipamento apresentar defeito por 2 (duas) ou mais vezes dentro de um período de 20 (vinte) dias corridos.

2.5.25. Caso os equipamentos cobertos pelo serviço de garantia, atualização de assinaturas de proteção e suporte técnico vierem a ser declarados pelo fabricante em listas de *end-of-life*, *end-of-support* e/ou *end-of-sale* com essas datas terminando antes do período de vigência do contrato, os mesmos deverão ser substituídos pelos novos equipamentos indicados pelo fabricante em seu site, esses equipamentos devem ter capacidade idêntica ou superior ao equipamento antigo e possibilitar o uso de todas as funcionalidades do equipamento anterior.

2.5.26. Os serviços dependentes de atualização pela Internet e cujas licenças serão vinculadas à vigência do contrato, são: controle de acesso à Internet (controle de aplicações e filtragem de URLs), SD-WAN, prevenção de ameaças (IPS, Antivírus, Anti-Bot, Anti-Malware, Anti-Spyware), prevenção de perda de dados (data loss prevention) e postura dos *endpoints*, e demais funcionalidades necessárias para completa utilização dos equipamentos.

2.5.27. O licenciamento deverá permitir a utilização da solução, por tempo indeterminado, em sua última versão disponível na data do encerramento dos serviços de garantia, suporte técnico e atualização de versões.

2.6. Vigência e início do contrato

Os serviços de garantia e suporte terão vigência de 60 meses, com início a partir da emissão do termo de recebimento definitivo.

2.7. Itens 9 e 10 - Licenciamento de Serviço de *Software-Defined* WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls Tipo I e Tipo IV e dos itens 2 e 7 - Firewalls Tipo II e Tipo V

A solução de *Software-Defined* WAN (SD-WAN) deverá ser licenciada de forma a garantir um canal de comunicação seguro, utilizando a Internet, para conectar os Firewalls Centrais (em configuração de Cluster, dos tipos I, II, IV, V) aos Firewalls menores (dos tipos VI, VII e VIII).

Apesar de a compatibilidade do serviço de SD-WAN abranger os Firewalls dos tipos I, II, III, IV, V, VI, VII e VIII (Grupo I Itens 1 a 7 e Grupo II itens 11 a 13 do Edital), a habilitação desse serviço — seja por meio de licença ou componente de hardware adicional — aplica-se apenas aos Firewalls dos tipos I, II, IV e V. Isso ocorre porque os equipamentos dos tipos VI, VII e VIII (Itens 11 a 13 do Edital) já devem ter o serviço de SD-WAN ativado por padrão, sem a necessidade de aquisição separada. Já para o firewall tipo III não está prevista licença SD-WAN.

Uma unidade do Item 9 ou 10 corresponderá ao licenciamento SD-WAN para um cluster de equipamentos correspondente.

2.7.1. Vigência e início do contrato

Os serviços definidos nos itens 9 e 10 terão vigência de 60 meses, com início a partir da emissão do termo de recebimento definitivo da licença.

2.7.2. Requisitos mínimos para serviço de *Software-Defined* WAN (SD-WAN)

2.7.2.1. Após a solicitação do contratante a empresa terá até 15 dias para fornecer/habilitar o serviço.

2.7.2.2. A solução de SD-WAN deve ser parte da solução de segurança, com políticas comuns ao firewall principal, gerência e logs centralizados.

2.7.2.3. A solução deve permitir conexão entre os Firewalls via túnel criptografado (VPN *site-to-site*)

2.7.3. A solução deve permitir ao usuário da unidade remoto acesso à Internet diretamente, sem passar pelo Firewall principal da contratante, mas com as mesmas políticas de segurança, inspeção e filtro de conteúdo, de acordo com o seu perfil;

3. Grupo III - Solução de SASE (*Secure Access Service Edge*) e ZTNA (*Zero Trust Network Access*) na modalidade *Software* como serviço e Treinamento

Esta seção trata das especificações do grupo III itens 14 e 15 para a Solução de SASE (*Secure Access Service Edge*) e ZTNA *Zero Trust Network Access*.

3.1. Grupo III item 14 Licença de uso de solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access) por usuário pelo período de 60 meses.

3.1.1. Características Gerais

3.1.1.1. As licenças de uso do SASE devem estar disponíveis para uso, integrada com a base de identificação de usuários do contratante, em até 60 dias da comunicação da assinatura do contrato.

3.1.1.2. O contrato terá vigência de 60 meses.

3.1.1.3. Anualmente, na data de aniversário do contrato, a contratada poderá redefinir o número de contas ativas, respeitando o mínimo de 200 contas e o teto definido no contrato.

3.1.1.4. A quantidade de licenças que devem ser inicialmente ativadas será informada à contratada no início do contrato. Essa quantidade deverá ser de no mínimo 200 (duzentas) licenças ativas. A solicitação precisará ser registrada por, no mínimo, e-mail.

3.1.1.5. Caberá à Contratante fazer o primeiro contato com a Contratada para saber a quantidade de licenças que deve ser enviada no primeiro pedido;

3.1.1.6. Caso seja solicitada a ativação de uma quantidade de contas inferior à quantidade máxima contratada, a diferença entre a quantidade de licenças solicitadas (ativas) e a quantidade de licenças contratadas será o saldo de licenças disponíveis, que não serão consideradas como ativas;

3.1.1.7. A Contratante poderá solicitar à Contratada, ajuste na quantidade de licenças, em múltiplos de 10, dentro do limite de licenças disponíveis no contrato. As licenças solicitadas comporão o total de licenças ativas para os próximos 12 meses. Esse processo poderá ser refeito a cada 12 meses;

3.1.1.8. Os ajustes anuais deverão respeitar o piso de 200 licenças e o teto definido em contrato.

3.1.1.9. Se a Contratada fornecer quantidade de licenças diferente da solicitada pela Contratante, caberá a Contratada arcar com os custos para regularizar a situação. A regularização da situação deverá ocorrer em até 15 dias corridos, contados da notificação da contratante.

3.1.1.10. Para efeito de pagamento, a quantidade total de licenças solicitadas será considerada como a quantidade de licenças ativas. O pagamento corresponderá ao número de licenças ativas.

3.1.1.11. As licenças só serão consideradas entregues quando estiverem disponíveis no console de administração e em acordo com a quantidade total solicitada;

3.1.1.12. Cada novo reajuste do quantitativo de licenças ativas deverá ser atendido em até 5 (cinco) dias úteis.

3.1.1.13. O contrato terá pagamento referente ao número de licenças definido na data da assinatura de contrato, ou na revisão anual do quantitativo, será efetuado **mensalmente, após a efetiva prestação dos serviços**, mediante apresentação de

nota fiscal/fatura correspondente e atestado de conformidade emitido pelo contratante, referente aos 12 meses seguintes de licença.

3.1.1.14. Todas as funcionalidades deverão ser ofertadas em nuvem, como serviço e por meio de um único agente instalado na máquina do usuário. A nuvem deverá ser distribuída globalmente, incluindo o Brasil e deverá ser licenciada por usuário, conforme quantitativo definido por cada participante;

3.1.1.15. A plataforma de segurança deverá ter ponto de presença no Brasil (Data Center), onde todos os usuários em território nacional terão suas transações processadas, incluindo todas as inspeções e aplicação de políticas de controle de acesso e segurança em tempo real;

3.1.1.16. O Data Center localizado no Brasil deverá ter rede independente com Sistema Autônomo e conectividade, redundante, em PTT (Ponto de Troca de Tráfego) no Brasil com peering com provedores de serviços, empresas de telecomunicações, CDNs (*Content Delivery Network*) e provedores de nuvem pública tais como (AWS, Microsoft e Google). Desta forma garantindo a melhor experiência e baixa latência aos usuários.

3.1.1.17. Não serão aceitos para solução SASE sistemas baseados em hardware ou software projetados para uso genérico, ou de código aberto (*open source*).

3.1.1.18. A solução de SASE deverá suportar todas as funcionalidades descritas neste certame no que tange controle de acesso e segurança à Internet e a aplicações SaaS por meio das seguintes opções de arquitetura de conectividade à plataforma de segurança:

a) Agentes instalados nas máquinas, e;
b) Utilização de proxy explícito via arquivos PAC (Proxy Auto-Configuration), neste caso com funcionalidades limitadas a acesso Web HTTP, HTTPS.

3.1.1.19. A solução de segurança, proteção de dados, controle de acesso à Internet e aplicações deverá fornecer disponibilidade de 99.999% ao ano;

3.1.1.20. Suportar geração de logs detalhados de acesso dos usuários Web, Aplicações Cloud, Bloqueios de Segurança e acessos;

3.1.1.21. Todas as inspeções e aplicações de políticas deverão ser realizadas na nuvem. Com exceção da verificação de postura, nenhuma inspeção de controle de acesso ou segurança deverá ser realizada na máquina do usuário;

3.1.1.22. A solução de segurança, proteção de dados e controle de acesso à Internet deverá oferecer suporte à criação de múltiplos administradores com privilégios distintos e segmentados;

3.1.1.23. No caso da utilização de agentes, a gestão de como o tráfego será encaminhado à plataforma, incluindo eventuais exclusões específicas (*bypass*), deverá ser gerenciada de maneira centralizada em uma console Web com o contexto de usuário e grupos de usuários. Não serão aceitas soluções que requeiram alteração ou customizações diretamente na máquina do usuário;

3.1.1.24. O agente único deve ser compatível com no mínimo os seguintes sistemas operacionais:

a) Windows 10 ou superior;
b) Linux kernel 6.6 ou superior;
c) MacOS 13 ou superior;
d) IOS 16 ou superior, e;
e) Android 12 ou superior.

3.1.1.25. Toda a solução proposta deverá ser implementada com autenticação dos usuários integrada e suportar aplicações de políticas granulares com base em nome do usuário, e grupos, integrados com a plataforma Microsoft AD utilizando protocolo SAML (*Security Assertion Markup Language*) e LDAP via OpenLDAP;

3.1.1.26. A solução de segurança deverá realizar, em uma única plataforma, sem passar por inspeção em múltiplos componentes de rede dentro da nuvem do

fabricante ou de terceiros, os controles de acesso e proteção de segurança para acesso à Internet e aplicações SaaS, consolidando capacidades de soluções de SWG e FWaaS;

3.1.1.27. Os mecanismos de inspeção da plataforma (URL *filtering*, Antivírus, etc) devem verificar todo o conteúdo dos pacotes de forma simultânea e em uma única abertura;

3.1.1.28. A solução deverá integrar-se nativamente e enviar em tempo real logs para plataformas de SIEM (*Security Information and Event Management*) possibilitando a integração com, no mínimo, as soluções de SIEM IBM Qradar e Trend One, ferramentas que compõe a solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos que compõem a Ata de Registro de Preços n.20/2024, vigente, resultante do Pregão Eletrônico n.30/2024 - PROAD n. 22.093/2024 do TRT 2, contratada por vários órgãos participantes do presente processo;

3.1.1.29. A solução deve ser capaz de fornecer a visualização de logs em tempo real;

3.1.1.30. A solução deverá armazenar os logs de auditoria por no mínimo 3 meses;

3.1.1.31. Os logs de auditoria devem conter no mínimo:

a) Ação: Login, Criação, Deleção;
b) Interface utilizada: API, Console Administrativa, e;
c) Categoria: Gerenciamento, Controle de Acesso, Gerenciamento de funções, Controle de acesso Web, Segurança Web e configurações avançadas.

3.1.2. Características para funcionalidades de SWG (*Secure Web Gateway*)

3.1.2.1. Suportar inspeção de SSL/TLS em 100% do tráfego Web, sem limites de volume de transações ou percentual inspecionado, em protocolos TLS 1.2 e 1.3,

para acesso do cliente SASE e os protocolos TLS 1.0, 1.1, 1.2, 1.3 para acesso às aplicações internas disponibilizadas;

3.1.2.2. Possibilidade de criar regras granulares de exceção a inspeção SSL/TLS, com base categorias de URL, host e domínios de destino, usuário, grupo ou departamento;

3.1.2.3. A solução deverá identificar automaticamente tráfegos Web em portas não padrão (80 e 443) e realizar a inspeção Web completa, incluindo inspeção SSL/TLS e todas as funcionalidades de controle de acesso e segurança, mesmo em uma arquitetura de proxy transparente;

3.1.2.4. Capacidade de criar filtros de URLs com base em categorias e subcategorias, que deverão ser atualizadas constantemente pelo fabricante;

3.1.2.5. Suportar a criação de categorias customizadas;

3.1.2.6. Suportar a criação e manutenção listas de URL via API;

3.1.2.7. A solução deve fornecer mecanismo para bloquear o acesso Web a destinos hospedados em determinados países. Este bloqueio deverá ser configurado de maneira simples, apenas selecionando os países que deseja bloquear;

3.1.2.8. Suportar o idioma Português do Brasil em páginas de erro e bloqueio apresentadas aos usuários, além de permitir customização;

3.1.2.9. A solução deverá ter capacidade de criar políticas Web, granulares, com critérios utilizando nome do usuário, grupos, departamento, categorias de URL, localidades para liberação ou bloqueio de upload e/ou download de arquivos de acordo com o seu tipo. Exemplo: EXE, RAR, PKG, XLS, PDF;

3.1.2.10. A solução deverá prover proteção de antivírus e antimalware com base em assinatura de arquivos. Esta proteção deverá ser realizada para download e upload, e a base de dados de assinatura ser atualizada constantemente pelo fabricante;

3.1.2.11. A solução deverá fornecer proteção contra ameaças avançadas, utilizando análise estática com base em reputação do domínio, origem, idade do domínio entre outras variáveis, além de uma análise dinâmica do conteúdo Web de 100% das requisições realizada a fim de detectar potenciais riscos aos usuários, tais como injeção de JavaScript malicioso, assinaturas de roubo de cookies XSS, conteúdos ativos maliciosos, conteúdos vulneráveis de ActiveX, Phishing dentre outras.

3.1.2.12. Deve possuir detecção e proteção de malwares para:

a) Todo tráfego Web de saída;
b) Inspeção dos seguintes protocolos: HTTP e HTTPS, e;
c) Adwares, Backdoor, Dialer, Downloader, Criptografado, Exploit, Hacktool, Heuristic, Keylogger, Infostealer, Packed, Potentially un-wanted applications, ransomware, rootkit, Spyware, Virus, Trojans e Worms.

3.1.2.13. A solução deverá ter atualizações constantes, minimamente diárias, de base de dados utilizada para bloqueio de segurança com base em reputação, prevenção a fraudes como Phishing, botnets, Command and Control, malware, spyware ou qualquer outro tipo de conteúdo malicioso;

3.1.2.14. A solução deverá detectar e bloquear assinaturas de ataques XSS (Cross Site Scripting) e de roubo de cookies dos usuários;

3.1.2.15. A solução deve monitorar e avaliar aplicações de comunicações unificadas, assim como o Teams e Zoom.

3.1.3. Características para funcionalidades de FWaaS (*Firewall as a Service*)

3.1.3.1. A solução deverá suportar capacidades de Firewall como serviço via agentes instalados nas máquinas dos usuários nas plataformas Windows, Linux, IOS, MacOS e Android;

3.1.3.2. A solução deve suportar, no mínimo, 350Mbps por túnel IPSEC;

3.1.3.3. Toda a inspeção e aplicação de política de Firewall, independente do método de implantação, deverá ser realizada na nuvem;

3.1.3.4. A solução deverá suportar a criação de regras de Firewall utilizando Destino, Protocolo udp/tcp e porta;

3.1.3.5. A solução deverá suportar como destino IP, Subredes ou endereços completos (FQDN);

3.1.3.6. A solução deverá suportar a criação de políticas de Web bloqueando o acesso a destinos em países específicos;

3.1.3.7. A solução deverá suportar criar regras, nos dois métodos de implementação com túneis ou agentes, com base em metadados do IdP como nome do usuário, grupos e departamento;

3.1.3.8. O FWaaS deverá ter capacidade de inspeção na camada 7, fazendo uso de tecnologia de DPI (*Deep Packet Inspection*), ou similar que entregue o mesmo caso de uso, para identificar nos primeiros pacotes a aplicação que está sendo utilizada;

3.1.3.9. A solução de FWaaS deverá possuir a capacidade de criar políticas específicas granulares para proteção de DNS;

3.1.3.10. A solução deverá suportar políticas de proteção de DNS granulares contendo, no mínimo, metadados do IdP (usuário, grupos e departamento), Localidades, Origem e Domínios Destino;

3.1.3.11. Para a proteção de DNS a solução deverá permitir ações como bloqueio ou redirecionar para um IP de BOTNETS para página de bloqueio;

3.1.3.12. A solução deverá ter proteção nativa contra ataques de DNS *Tunneling* que permita bloqueio de destinos maliciosos conhecidos, além de conter mecanismo de

detecção de assinaturas de ataques utilizando ferramentas conhecidas de DNS Tunneling como iodine, independente do domínio utilizado;

3.1.3.13. A proteção de DNS deverá permitir bloqueio via DNS, independente do protocolo da aplicação, de domínios com baixa reputação ou com histórico de ser malicioso para *Phishing*, Conteúdo Malicioso e utilizados para Botnets;

3.1.3.14. A solução deverá detectar e redirecionar requisições de DNS utilizando DOH (DNS over HTTPS), de forma transparente, para aplicação de políticas de DNS, detalhadas nos itens acima, Serão aceitas soluções que bloqueiem o DOH e realizem apliquem as políticas da resolução de DNS tradicional;

3.1.3.15. Assim como todo o escopo do FWaaS, a solução de proteção de DNS deverá suportar a implementação via agentes instalados nos dispositivos dos usuários;

3.1.4. Características para funcionalidades de visibilidade e controle de aplicações

3.1.4.1. A solução deverá identificar automaticamente uso de aplicações em nuvem (Cloud) pelos usuários, criando visibilidade em Dashboards e relatórios de Shadow IT;

3.1.4.2. O relatório de Shadow IT deverá permitir identificar uso de aplicações não sancionadas e com risco elevado, além de visualizar pela própria interface Web da solução quais usuários estão utilizando estas aplicações;

3.1.4.3. A solução deverá suportar a identificação e classificação entre aplicações sancionadas e não sancionadas pela contratante de, no mínimo, 4600 aplicações distintas. Esta base de dados deverá ser mantida e constantemente atualizada pelo fabricante e deverá conter, no mínimo, a categoria da aplicação;

3.1.4.4. A solução deverá permitir a criação de políticas de acesso com base na classificação da aplicação SaaS realizada pela contratante entre sancionadas e não sancionadas e índice de risco da aplicação;

3.1.4.5. A solução deverá suportar criar políticas granulares com critérios utilizando usuário, grupo, departamento, localidade e ações específicas nas aplicações SaaS. Como por exemplo, aplicações de compartilhamento de arquivos ter as opções de *Upload* e *Download* como critério, em aplicações como Webmail, ter as opções de Leitura e Envia de e-mails como critério;

3.1.5. Características para funcionalidades de Monitoramento da Experiência do Usuário

3.1.5.1. A solução deverá realizar monitoramento sintético a partir da máquina do usuário final, com testes de página Web e de Rede;

3.1.5.2. A console de gerenciamento deverá ser Web, e ter toda a configuração de forma centralizada;

3.1.5.3. A execução dos testes não deverá impactar o usuário final e deverá ser realizada em segundo plano, sendo transparente e imperceptível;

3.1.5.4. Quando executado testes de Web e Rede da mesma aplicação, por exemplo, Microsoft Teams, a solução deverá consolidar as métricas e apresentar uma única visão da experiência do usuário ao utilizar a aplicação SaaS;

3.1.5.5. A solução deverá apresentar Dashboards com o status das aplicações;

3.1.5.6. A Geolocalização deverá ser feita de maneira automática e transparente, sem nenhuma entrada de dados manual;

3.1.5.7. Caso o usuário esteja dentro de localizações conhecidas da solução de SWG e FWaaS, a solução deverá identificar que se trata de uma localidade conhecida;

3.1.5.8. Os testes e coleta de dados deverão acontecer no máximo a cada 15 (quinze) minutos;

3.1.5.9. A solução deverá coletar no mínimo as seguintes métricas de experiência:

a) Métricas Web:
   i - Tempo de resposta do Servidor;

b) Métricas do dispositivo do usuário:
   i - Consumo de CPU;
   ii - Qualidade do sinal Wi-Fi;
   iii - Memória;
   iv - Sistema Operacional, Descrição do hardware, IP público e IP externo utilizado;

3.1.5.10. Utilizando as métricas do dispositivo do usuário, a solução deverá ter um mecanismo simples de identificar a experiência do usuário em uma aplicação;

3.1.5.11. A solução deverá suportar o monitoramento de Websites na Internet e aplicações SaaS;

3.1.5.12. A solução deverá suportar a criação de alertas customizáveis com notificação por email;

3.1.5.13. A solução deverá manter o histórico da experiência de todos os usuários, por no mínimo 24 (vinte e quatro) horas;

3.1.6. Acesso a Aplicações Privadas

3.1.6.1. A solução deverá fornecer acesso remoto a aplicações e recursos internos da contratante, com segurança, validação de identidade, tunelamento encriptado, segregação de aplicações, verificação de postura e conexão direta com privilégio mínimo;

3.1.6.2. Deve permitir a conexão de no mínimo 500 usuários remotos de forma simultânea por órgão participante;

3.1.6.3. A solução deve habilitar uma arquitetura de privilégio mínimo, Zero Trust, definindo uma política de acesso granular para fornecer às pessoas certas no contexto certo, o acesso menos privilegiado aos aplicativos ou recursos e reduzir a superfície de ataque.

3.1.6.4. A solução deverá ser na nuvem e ter apenas o componente que irá viabilizar a conexão (conector ou publicador) instalado dentro do Data Center da contratante em uma, ou mais, máquinas virtuais.
Este componente interno ao Data Center deve seguir as seguintes características:

a) Não ter uma superfície de ataque exposta na Internet, não tendo nenhum IP público ou nenhuma necessidade de conexões de entrada da Internet para o componente;
b) Toda a conexão deverá ser apenas de saída, do componente com destino a nuvem do fabricante;
c) Cada instância de conector ou publicador deverá suportar no mínimo 500mbps de banda passante para acesso às aplicações internas;
d) Os conectores ou publicadores deverão atualizar suas versões de forma automática e realizar suas atualizações em janelas pré-definidas pela contratante (ex: Domingo às 4 AM) de forma 100% automatizada, sem causar interrupção dos serviços e sem intervenção do administrador;
e) Permitir ser instalado de forma flexível em qualquer ponto da rede da contratante, como por exemplo atrás de uma NAT (*Network Address Translation*);
f) Não criar um ponto único de conexão à rede da contratante, sendo possível a implementação de múltiplos conectores ou publicadores em pontos da rede, data centers ou nuvem distintas, fornecendo ao usuário o acesso direto aos recursos com menor latência possível de forma dinâmica;
g) Permitir o usuário a conectar em aplicações distintas simultaneamente utilizando conectores ou publicadores em pontos da rede distintos, priorizando sempre a melhor experiência do usuário;
h) Os conectores ou publicadores deverão ser independentes, não exigindo conectividade interna completa a todos os recursos privados. Sendo possível,

por exemplo, fornece acesso a aplicações ou recursos simultaneamente aos usuários em múltiplos Data Centers ou Nuvem, mesmo que estes Data Centers ou Nuvem não tenham conexão entre eles, e;

i) A solução deverá autenticar o usuário em um provedor de identidade (IdP) e com base em identidade, políticas granulares, segmentação de aplicações e posturas específicas fornecer acesso a aplicações Web, ou qualquer outra com protocolo TCP e UDP, tais como (SSH, RDP, SQL, Aplicações Client-to-Server, Compartilhamento de Arquivos, etc) de forma transparente, sem a necessidade de alteração do cliente original da aplicação, criando um túnel encriptado que conectará o usuário até a aplicação e não a rede da contratante.

3.1.6.5. A solução não deve operar como uma VPN, fornecendo um IP da rede local, e sim, conectar o usuário direto aos recursos e aplicações via túneis encriptados específicos, sempre após validação de política de identidade, postura e políticas de acesso;

3.1.6.6. Os usuários remotos não devem possuir visibilidade de aplicativos não autorizados. Os recursos não autorizados não devem apenas ser inacessíveis, mas também completamente invisíveis;

3.1.6.7. A definição de aplicações ou segmentos de aplicações deverá ter a flexibilidade de suportar hostname (FQDN), IP ou domínio com wildcard, como por exemplo (*.rede.local)

3.1.6.8. Fazer com que cada solicitação do usuário flua por meio de políticas contextuais para autenticação e autorizações consistentes, além de fornecer um ponto de monitoramento e registro unificado;

3.1.6.9. Utilizar túneis encriptados TLS ou DTLS, versão 1.2 ou 1.3;

3.1.6.10. Todas as comunicações entre os componentes da solução e a infraestrutura em nuvem do fabricante devem mutuamente utilizar certificados pinados ou IPSEC;

3.1.6.11. A solução deve ser blindada contra-ataques de “Man-in-the-middle” (MITM), aceitando-se que a blindagem contra MITM seja via IPSEC;

3.1.6.12. Suportar múltiplos provedores de identidade (IdP - Identity Provider) e múltiplos domínios, na mesma instância e console de gestão, que suporte autenticação utilizando protocolo SAML 2.0 e LDAP. Viabilizando desta forma, acesso seguro a outras unidades de negócio e terceiros a recursos privados da contratante, além de possibilitar a simplificação e modernização da conectividade e integrações futuras;

3.1.6.13. Permitir a descoberta automatizada de novas aplicações que não foram previamente provisionadas aos usuários explicitamente;

3.1.6.14. Trazer o monitoramento da atividade dos usuários, dando às equipes de TI formas de monitorar e gerenciar facilmente todas as atividades de forma granular, entendendo, no mínimo, qual usuário, quando, qual aplicação, qual política autorizou ou negou o acesso, status da postura e localização do usuário;

3.1.6.15. A solução deverá suportar envio, em tempo real, das informações do item anterior para uma plataforma de SIEM, possibilitando a integração com, no mínimo, as soluções de SIEM IBM Qradar e Trend One, ferramentas que compõe a solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos que compõem a Ata de Registro de Preços n.20/2024, vigente, resultante do Pregão Eletrônico n.30/2024 - PROAD n. 22.093/2024 do TRT 2, contratada por vários órgãos participantes do presente processo;

3.1.6.16. A solução deve usar o painel Web para criar e editar políticas com facilidade. O portal de gestão central deve trazer:

a) Controle de acesso centralizado;
b) Gestão de políticas;
c) Configuração de postura;

d) Registro de atividades detalhados e seus metadados contendo, no mínimo, usuário, localidade, postura, IP de origem, aplicação destino, política de acesso que concedeu ou negou o acesso;
e) Status da estrutura que suporte a solução como conectores ou publicadores;
f) Status do processo de atualização automatizada dos conectores e publicadores, e;
g) Status das aplicações que deverão ser monitoradas e se estas estão disponíveis ou não.

3.1.6.17. Suportar a configuração de qualquer aplicação TCP ou UDP com tráfego originado pelo usuário de forma transparente, sem nenhuma alteração ou customização no seu cliente original;

3.1.6.18. Permitir o agrupamento de aplicações ou recursos para facilitar a criação de políticas (ex: Aplicações Administrativas);

3.1.6.19. Suportar a gestão de políticas de acesso via API;

3.1.6.20. Suportar diferentes tipos de validação de postura. O suporte a cada tipo pode variar dependendo da plataforma (Windows, Mac, Linux), sendo requerido que deverá suportar, no mínimo, 2 (dois) dos tipos de postura listadas abaixo por plataforma:

a) Validação da presença de um Antivírus;
b) Validação de Certificado Cliente (chave privada e pública) assinada por um CA específico;
c) Validação de Certificado confiável no dispositivo;
d) Validação de qualquer processo executando na máquina, incluindo a validação da assinatura do seu fabricante;
e) Validação de máquina no domínio;
f) Validação de disco encriptado;
g) Validação de Registro de chave no Windows, e;
h) Validação de presença de um arquivo.

3.1.6.21. Exigência de uma versão mínima do Sistema Operacional;

3.1.6.22. Detectar alterações Jail Break (IOS) e rooted (Android).

3.1.6.23. A solução deverá ter mecanismos de proteção e políticas granulares de postura para cada acesso à aplicação. Desta maneira permitindo criar maiores restrições a aplicações mais críticas ao negócio e menos restritas a aplicações de suporte a TI.

3.1.7. Ferramenta de iscas digitais (Deception)

3.1.7.1. A solução deve possuir módulo de defesa ativa para detecção de ameaças na rede interna e externa;

3.1.7.2. Exclusivamente para o módulo de defesa ativa será aceita composição de soluções terceiras para o completo atendimento;

3.1.7.3. A solução proativa deve ser capaz de espalhar iscas no ambiente a fim de enganar o atacante;

3.1.7.4. A solução deve permitir a instalação de um conector no ambiente da contratante capaz de criar “iscas” falsas em várias redes locais (VLAN’s);

3.1.7.5. Possuir iscas de rede capazes de detectar atividades de varredura e movimentação lateral;

3.1.7.6. Permitir a instalação de agentes nos Endpoints da contratante possibilitando a criação de arquivos, processos e credenciais falsas;

3.1.7.7. Capacidade de” imitar” ativos reais da rede a fim de enganar o atacante;

3.1.7.8. A solução deve ser licenciada para no mínimo 20 Iscas/Chamarizes ou VLANs;

3.1.7.9. Possuir, pelo menos, os seguintes tipos de Iscas/Chamarizes:

a) Iscas de Rede: Espalhadas em segmentos de rede específicos;
b) Iscas no Active Directory: Criação de usuário e computadores falsos, e;
c) Iscas nos Endpoints: Criação de arquivos, aplicações e credenciais falsas.

3.1.7.10. Deve ser capaz de mostrar um sumário de todas as iscas espalhadas dentro do ambiente e o status de operação;

3.1.7.11. Deve possuir Iscas de inteligência externas que devem ser apontadas no DNS externo da contratante;

3.1.7.12. A solução deve ser capaz de detectar e mapear ocorrências de acordo com framework MITRE ICS.

3.1.7.13. O módulo de defesa ativa deve fornecer uma visão geral de forma temporal das atividades detectadas pela plataforma;

3.1.7.14. A solução deve fornecer uma visão geral temporal das atividades detectadas ao longo do tempo e ao longo da semana;

3.1.7.15. Deve permitir analisar eventos passados permitindo customização da janela de tempo;

3.1.7.16. A solução deve fornecer uma barra de consulta usada para filtrar os eventos detectados pela plataforma;

3.1.7.17. Dentre as formas de pesquisa a solução deve ser capaz de filtrar no mínimo as seguintes informações:

a) Endereço IP do Atacante;
b) IP de Destino;
c) Porta de destino;
d) Duração da conexão;
e) Score de Risco do atacante;

f) Protocolo de rede;
g) Fase do Kill Chain, e;
h) Tipo da isca;

3.1.7.18. A solução deve ser capaz de exportar evidências coletadas pelas iscas em pelo menos um dos seguintes formatos:

a) RDP;
b) IOCs;
c) PCAP e;
d) STIX, que é um padrão para representar e compartilhar informações sobre ameaças cibernéticas de forma estruturada e automatizada.

3.2. Item 15 - Voucher de Treinamento para solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access)

3.2.1. O Treinamento fornecerá uma compreensão dos conceitos básicos e das habilidades necessárias para configurar o sistema previsto no item 17 do Edital da presente licitação.

3.2.2. O curso deverá abordar configurações de políticas de SASE (*Secure Access Service Edge*) e ZTNA (*Zero Trust Network Access*), gerenciamento e monitoramento da solução, atualizações e configurações de soluções de SASE e ZTNA.

3.2.3. O Treinamento deverá ser fornecido na forma de voucher[6] individual para treinamento;

3.2.4. A duração do treinamento deve ser de, no mínimo, 20 horas aula distribuídas em até 5 dias úteis, com um máximo de 8 horas aula por dia;

[6] Para o objeto definido nos itens 8 e 15 da presente contratação, o Voucher é um vale, ou valor em crédito, para realização de Treinamento dentro de plataforma de educação à distância, que deve ser disponibilizado em turmas regulares dentro de um período específico de tempo.

3.2.5. O treinamento e o material didático deverão ser em língua portuguesa;

3.2.6. O treinamento deverá ocorrer no período entre 8h00 e 18h00;

3.2.7. As turmas deverão ter até 15 alunos;

3.2.8. O treinamento deverá ser realizado de forma on-line e síncrona;

3.2.9. Deverá ser fornecido certificado de conclusão do treinamento em até 10 dias após sua conclusão, contendo:

a) Nome do Aluno;
b) Nome do Curso;
c) Carga horária do Curso;
d) Data de início e fim do Curso;
e) Nome e assinatura do emissor, e;
f) Linguagem em Português do Brasil. Mesmos os certificados oficiais do fabricante.

3.2.10. As turmas para os cursos devem estar disponíveis para as contratantes em até 30 dias corridos após a comunicação da assinatura de cada contrato de aquisição de vouchers.

3.2.11. Devem haver turmas regulares até 12 meses depois da data da comunicação da assinatura de cada contrato.

3.2.12. A contratante deve ser comunicada mensalmente das turmas regulares e pode comunicar o uso do voucher do curso até, no mínimo, 15 dias antes do início da turma.

3.2.13. Conteúdo programático:

a) Características e funcionalidades básicas da solução;
b) Funcionalidades e operação de SWG (Secure Web Gateway);

c) Funcionalidades e operação de FWaaS(Firewall as a Service);
d) Visibilidade e controle de aplicações;
e) Configuração e análise da Experiência do Usuário;
f) Acesso e configuração das aplicações privadas, e;
a) Configuração de ZTNA, configuração de políticas de postura para clientes Windows e Linux. Substituição de VPN cliente por ZTNA benefícios e diferença entre os conceitos.

4. Grupo IV - Serviço Gerenciado Mensal

4.1. Itens 16, 17 e 18 - Serviço gerenciado mensal, contendo operação assistida, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos Grupo I (itens 1, 4 e 6) - Tipo I e Tipo IV, Grupo I (itens 2 e 7) - Tipo II e Tipo V e Grupo I (itens 3 e 5) - Tipo III

Especificação completa dos itens 16 a 18, Serviço Gerenciado com tratamento de incidentes para Cluster de equipamentos do Tipo I, II, III, IV e V.

Importante: Para contratar o serviço gerenciado, o órgão deve, obrigatoriamente, possuir/adquirir o cluster correspondente com suporte e garantia ativos (Itens 1 a 7).

Entende-se também apropriado apresentar um único conjunto de especificações para os serviços gerenciados dos itens 16 a 18 porque, neste processo, a diferença entre estes itens é o tipo de equipamentos em que o serviço será aplicado, conforme segue:

- Item 16 - Cluster de equipamentos do Grupo I (itens 1, 4 e 7) - Tipo I e Tipo IV;
- Item 17 - Cluster de equipamentos do Grupo 1 (itens 2, 5 e 8) - Tipo II e Tipo V;
- Item 18 - Cluster de equipamentos do Grupo I (itens 3 e 6) - Tipo III;

Como cada serviço gerenciado é ligado a um tipo/grupo de equipamentos, caso o Órgão participante possua mais de um Cluster de equipamentos Firewall deverá adquirir quantitativo de mais de um item do grupo.

4.1.1. Serviço Gerenciado de Administração, Operação e Suporte da Solução

4.1.1.1. Características Gerais

Os serviços gerenciados devem fornecer suporte técnico avançado em segurança de redes para solução de Firewall de próxima geração, de forma pró ativa, ou seja, tomando a iniciativa de ajustes e combate a invasões, em regime 24x7 (vinte quatro horas por dia e sete dias por semana), incluindo finais de semana e feriados).

O serviço tem especial valor por conter monitoramento e possibilidade de atuação quando não há equipe do contratante em operação, ou seja, fora do expediente.

A contratada deve atuar, no mínimo, nas seguintes situações:

a) Ataques de dia zero (*zero-day*);
b) Extração de ameaças;
c) Antivírus;
d) Anti-bot;
e) IPS;
f) Controle de aplicativos;
g) Filtragem de URL e reconhecimento de identidade, e
h) SD-WAN (quando a contratada adquirir o item 11,12 e/ou 13).

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.

4.1.1.2 O serviço gerenciado para atendimento de ocorrências deve acontecer no regime 24x7x365. Ou seja, 24 horas por dia, sete dias por semana, 365 dias por ano, incluindo feriados;

4.1.1.3. Monitoramento remoto do ambiente do contratante em regime 24x7 através de plataforma de gerência do fabricante, com, no mínimo:

a) Tratamento de falsos positivos e de falsos negativos;
b) Interpretação de resultados em análises de detecções;
c) Emissão de relatórios técnicos e executivos contemplando, ao menos, o nível de aderência à solução e ameaças detectadas;
d) Análise forense dos eventos adversos que ocorrerem e forem detectados pela solução;
e) Atuação na investigação e contenção de ameaça relacionada à detecção de evento adverso;
f) Envolvimento da equipe técnica da contratante no tratamento de eventos adversos.

4.1.1.4. Relatórios com frequência mensal apresentando, no mínimo:

a) O diagnóstico do sistema de Firewall (*health check*);
b) Resumo dos chamados tratados no mês, e;
c) A listagem dos últimos acessos de nível administrativo.

4.1.1.5. Requisição de Mudança para configuração de Regras e Criação de Redes Virtuais Privadas (VPN);

4.1.1.6. Atualização de Firmware dos equipamentos[7];

4.1.1.7. Auxílio na substituição de produtos[8];

[7] Desde que haja contrato de atualização do produto vigente e em nome do contratante.
[8] Desde que haja contrato de suporte do fabricante, prevendo troca de equipamentos, vigente e em nome do contratante.

4.1.1.8. Prever, no mínimo, 10 horas por mês de Serviço de suporte de nível 2 e 3 do fabricante.

4.1.1.9. Deve contemplar atuação pró-ativa, por meio da administração e operação diária da solução e pelo contato entre as equipes técnicas da contratada e da contratante, enquanto a atuação reativa será realizada por meio da abertura de chamados pela equipe técnica da contratante, para os quais contarão os Níveis Mínimos de Serviço;

4.1.1.10. Os métodos de atuação serão acessos remotos e efetuados via VPN fornecida pelo contratante;

4.1.2. Vigência e início do contrato

Os serviços gerenciados terão vigência de 60 meses, iniciando em até 15 dias da comunicação da assinatura do contrato.

4.2. Item 19 - Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) - Tipo VI, Tipo VII e Tipo VIII

4.2.1. Serviço Gerenciado de Administração, Operação e Suporte da Solução com resposta a incidentes

4.2.1.1. Características Gerais

Os serviços gerenciados devem fornecer suporte técnico avançado em segurança de redes para solução de Firewall de próxima geração nos equipamento do Tipo VI, VII e VIII, de forma pró ativa, ou seja, tomando a iniciativa de ajustes e combate a invasões, em regime 24x7 (vinte quatro horas por dia e sete dias por semana, incluindo finais de semana e feriados).

O serviço tem especial valor por conter monitoramento e possibilidade de atuação quando não há equipe do contratante em operação, ou seja, fora do expediente.

A contratada deve atuar, no mínimo, nas seguintes situações:

a) Ataques de dia zero (*zero-day*);
b) Extração de ameaças;
c) Antivírus;
d) Anti-bot;
e) IPS;
f) Controle de aplicativos;
g) Filtragem de URL e reconhecimento de identidade, e;
h) SD-WAN

4.2.1.2. O serviço gerenciado para atendimento de ocorrências deve acontecer no regime 24x7x365. Ou seja, 24 horas por dia, sete dias por semana, 365 dias por ano, incluindo feriados;

4.2.1.3. Monitoramento remoto do ambiente do contratante em regime 24x7 através de plataforma de gerência do fabricante, com, no mínimo:

a) Tratamento de falsos positivos e de falsos negativos;
b) Interpretação de resultados em análises de detecções;
c) Análise dos eventos relacionados a rede SD-WAN, com fornecimento de soluções ou melhorias dos controles aplicados;
d) Emissão de relatórios técnicos e executivos contemplando, ao menos, o nível de aderência à solução e ameaças detectadas;
e) Análise forense dos eventos adversos que ocorrerem e forem detectados pela solução;
f) Atuação na investigação e contenção de ameaça relacionada à detecção de evento adverso, e;
g) Envolvimento da equipe técnica da contratante no tratamento de eventos adversos.

4.2.1.4. Relatórios com frequência mensal apresentando, no mínimo:

a) O diagnóstico do sistema de SD-WAN (*health check*);
b) Resumo dos chamados tratados no mês, e;
c) A listagem dos últimos acessos de nível administrativo.

4.2.1.5. Requisição de Mudança para configuração de Regras e Criação de Redes Virtuais Privadas (VPN).

4.2.1.6. Atualização de Firmware dos equipamentos[9].

4.2.1.7. Auxílio na substituição de produtos[10];

4.2.1.8. Deve contemplar atuação pró-ativa, por meio da administração e operação diária da solução e pelo contato entre as equipes técnicas da contratada e da contratante, enquanto a atuação reativa será realizada por meio da abertura de chamados pela equipe técnica da contratante, para os quais contarão os Níveis Mínimos de serviço;

4.2.1.9. Os métodos de atuação serão acessos remotos e efetuados via VPN fornecida pelo contratante;

4.2.1.10 O serviço deverá ser prestado em língua portuguesa.

4.2.2. Vigência e Início do Contrato

Os serviços gerenciados terão vigência de 60 meses, iniciando em até 15 dias da comunicação da assinatura do contrato.

4.3. Nível Mínimo de Serviço Para o Grupo IV - Serviço gerenciado mensal para equipamentos Firewall (Itens 16 a 19)

[9] Desde que haja contrato de atualização do produto vigente e em nome do contratante.
[10] Desde que haja contrato de suporte do fabricante, prevendo troca de equipamentos, vigente e em nome do contratante.

Os Níveis Mínimos de Serviço e severidades dos chamados para os Grupo IV, itens 16 a 19 são definidos na tabela TR5, a saber:

Tabela A5 - Níveis Mínimos de Serviço para Serviço Gerenciado

Severidade	Descrição	Prazo de Início de atendimento	Desconto por descumprimento (3)	Prazo de solução	Desconto por descumprir (3)
1 - Alta	Indisponibilidade total da solução, problema generalizado no ambiente tecnológico causado pela solução	2 horas a contar da abertura do chamado	1 % de desconto por hora adicional, limitado a 6 horas de atraso.	6 horas a contar da abertura do chamado	1% de desconto por hora adicional, limitado a 24 horas de atraso.
2 - Média	Falha, simultânea ou não, de uma ou mais funcionalidades, que não cause indisponibilidade, mas que apresente problemas de funcionamento e/ou desempenho da solução ou no ambiente tecnológico	4 horas a contar da abertura do chamado	0,2% de desconto por hora adicional, limitado a 24 horas de atraso.	NBD(1) + 1 dia útil (2)	0,2% de desconto por hora adicional, limitado a 96 horas de atraso.
3 - Baixa	Instalações, configurações, atualizações de versões, dúvidas dentre outros	NBD	0,1% de desconto por hora adicional, limitado a 48 horas de atraso.	NBD + 2 dias úteis	0,1% de desconto por hora adicional, limitado a 192 horas de atraso.

(1) NBD é uma sigla em inglês que significa Next Business Day, ou seja, próximo dia útil. (2) Serão considerados dias úteis todos os dias, com exceção de sábados, domingos e feriados nacionais. (3) O valor de referência para o desconto será o valor mensal pago pelo conjunto do serviço gerenciado. (4) A medição dos Níveis mínimos de serviço será feita mensalmente.

A contratante, a seu critério, poderá fornecer seu login e senha de acesso ao site do fabricante para que a equipe técnica da contratada possa responder pelo Regional nas interações referentes à garantia dos equipamentos. Nesses casos, a contagem do tempo de atendimento estipulada em contrato deverá ser suspensa, quando o chamado depender de ação do fabricante, especialmente quando for necessária a troca de equipamentos, a fim de evitar prejuízo por atraso que não seja de responsabilidade da contratada.

A impossibilidade de registro de chamados em qualquer horário contratado deverá ser considerada descumprimento do nível mínimo de serviço com severidade 1.

MALOTE DIGITAL

Tipo de documento: Administrativo

Código de rastreabilidade: 512202525974315

Nome original: 5 - Anexo II - Quantitativos para os Tribunais do Trabalho.pdf

Data: 19/08/2025 17:16:35

Remetente:

Tecnologia da Informação

Tecnologia da Informação

Tribunal Regional do Trabalho da 12ª Região

Documento: não assinado.

Prioridade: Normal.

Motivo de envio: Para conhecimento.

Assunto: Concordância dos órgãos participantes com os Estudos Técnicos Preliminares e Termo de Referência do registro de preços para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall.

Anexo II - Quantitativos dos itens dos participantes da aquisição de Solução de NG Firewall coordenada pelo TRT12 em 2025

ROBSON CLEITON NOVAK
17/03/2026
NGSI

		NG Firewall JT 2025 - Órgãos Participantes																					
		TST		TRT1		TRT3		TRT4		TRT5		TRT6		TRT7		TRT9		TRT10		TRT11		TRT12	
Item	Descrição	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo I - Pagamento em parcela única, antecipada.			1	1	1	1			1	1	1	2	1	1					1	1		
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo II - Pagamento em parcela única, antecipada.															1	1	1	2			1	1
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo III - Pagamento em parcela única, antecipada.																						
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo I - Pagamento em 5 parcelas fixas anuais.																						
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo III - Pagamento em 5 parcelas fixas anuais.																						
6	Aquisição de Cluster (...) - Tipo IV - Pagamento em parcela única, antecipada.	1	1																				
7	Aquisição de Cluster(...) - Tipo V - Pagamento em parcela única, antecipada.							1	1									1	2				
8	Voucher de Treinamento para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall	5	10	1	5	1	1	2	6	1	10	2	4	1	3	1	4	2	5	5	7	1	6
9	Licenciamento de Serviço de SD-WAN compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls Tipo I e Tipo IV									1	1			1	1								
10	Licenciamento de Serviço de SD-WAN compatível com os equipamentos NGFW dos itens 2, e 7 - Firewalls Tipo II e Tipo V																						

11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) (...) - Tipo VI									1	3												
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) (...) - Tipo VII									1	9			1	4								
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) (...) - Tipo VIII									1	21			1	15								
14	Licença de uso de solução de SASE e ZTNA por usuário pelo período de 60 meses			200	200			200	700	200	5600	200	400	200	1500	200	500	200	2500	500	1200	200	2500
15	Voucher de Treinamento para solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access)			1	5			1	5	1	10			1	10							1	6
16	Serviço gerenciado mensal (...) por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) - Tipo I e Tipo IV			1	1					1	1			1	1								
17	Serviço gerenciado mensa(...) por Cluster de equipamentos do Grupo I (itens 2 e 7) - Tipo II e Tipo V							1	2					1	1	1	1	1	2			1	1
18	Serviço gerenciado mensal (...) por Cluster de equipamentos do Grupo I (itens 3 e 5) - Tipo III																						
19	Serviço gerenciado mensal (...) por equipamentos do Grupo II (itens 11, 12 e 13) - Tipo VI, Tipo VII e Tipo VIII									1	33			1	15			1	18	15	15		

ROBSON
CLEITON
NOVAK
17/03/2026
NGSI

		NG Firewall JT 2025 - Órgãos Participantes																					
		TRT13		TRT14		TRT15		TRT16		TRT17		TRT18		TRT19		TRT20		TRT21		TRT22		TRT23	
Item	Descrição	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo I - Pagamento em parcela única, antecipada.	1	1			1	1									1	1	1	1				
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo II - Pagamento em parcela única, antecipada.											1	1									1	1
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo III - Pagamento em parcela única, antecipada.			1	1					1	1			1	1								
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo I - Pagamento em 5 parcelas fixas anuais.							1	1											1	1		
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo III - Pagamento em 5 parcelas fixas anuais.																						
6	Aquisição de Cluster (...) - Tipo IV - Pagamento em parcela única, antecipada.																						
7	Aquisição de Cluster(...) - Tipo V - Pagamento em parcela única, antecipada.																						
8	Voucher de Treinamento para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall	6	6			1	2	1	5	1	2	1	7	1	3	2	4	2	2	1	5	1	3
9	Licenciamento de Serviço de SD-WAN compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls Tipo I e Tipo IV																	0	0				
10	Licenciamento de Serviço de SD-WAN compatível com os equipamentos NGFW dos itens 2, e 7 - Firewalls Tipo II e Tipo V																						
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) (...) - Tipo VI																						
12	Equipamento Next Generation Firewall																						

ROBSON CLEITON NOVAK
17/03/2026
NGSI

	(appliance SDWAN e funcionalidades agregadas) (...) - Tipo VII																						
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) (...) - Tipo VIII																						
14	Licença de uso de solução de SASE e ZTNA por usuário pelo período de 60 meses	200	2000	200	1000	200	4500	200	1000			200	2300	200	200	200	400	200	1700				
15	Voucher de Treinamento para solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access)	6	6	1	4	2	15	1	10			1	7	1	5	2	4	3	7				
16	Serviço gerenciado mensal (...) por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) - Tipo I e Tipo IV					1	1	1	1							1	1	1	1				
17	Serviço gerenciado mensa(...) por Cluster de equipamentos do Grupo I (itens 2 e 7) - Tipo II e Tipo V											1	1										
18	Serviço gerenciado mensal (...) por Cluster de equipamentos do Grupo I (itens 3 e 5) - Tipo III			1	1					1	1			1	1								
19	Serviço gerenciado mensal (...) por equipamentos do Grupo II (itens 11, 12 e 13) - Tipo VI, Tipo VII e Tipo VIII																						

ROBSON
CLEITON
NOVAK
17/03/2026
NGSI