**Poder Judiciário Federal**
**Tribunal Regional Eleitoral de Pernambuco**

**ANEXO I**

**EDITAL DO PREGÃO N.º 73/2022 – ELETRÔNICO**

**REGISTRO DE PREÇOS**

**TERMO DE REFERÊNCIA**

## 1 - DO OBJETO

1.1 - Aquisição de firewall com software de análise de logs, conexão 2FA para VPN e suporte/garantia de 60 meses, conforme especificado abaixo:

**LOTE 1: Lote destinado a equipamentos de menor porte que atenderão a TRE's que possuem uma vazão de internet pequena, próxima a 2,3 Gbps, e uma vazão de núcleo também pequena, próxima a 3,6 Gbps.**

| ITENS | QUANTIDADE TRE-AM | QUANTIDADE TRE-RO | QUANTIDADE TRE-AP | QUANTIDADE TRE-PA | QUANTIDADE TOTAL PARA O LOTE |
|---|---|---|---|---|---|
| ITEM 1 - FIREWALL DE BORDA TIPO I | 02 | 02 | 02 | 04 | 10 |
| ITEM 2 - FIREWALL DE NÚCLEO TIPO I | 02 | 02 | 02 | 00 | 06 |
| ITEM 3 - FIREWALL DE CARTÓRIO TIPO I | 0 | 30 | 15 | 150 | 195 |
| ITEM 4 - SOFTWARE DE GERENCIAMENTO E RELATÓRIO | 04 | 34 | 19 | 154 | 211 |
| ITEM 5 - IMPLANTAÇÃO COM HANDS ON | 02 | 02 | 02 | 02 | 08 |
| ITEM 6 - TREINAMENTO OFICIAL | 02 | 04 | 01 | 02 | 09 |

**LOTE 2: Lote destinado a equipamentos de maior porte que atenderão ao TRE-SP que possui uma vazão de internet e de núcleo informada próxima a 30 Gbps, muito acima dos demais TRE's.**

| ITENS | QUANTIDADE TRE-SP |
|---|---|
| ITEM 7 - FIREWALL DE BORDA TIPO II | 04 |
| ITEM 8 - FIREWALL DE NÚCLEO TIPO II | 02 |
| ITEM 9 - FIREWALL DE NÚCLEO TIPO III (Exclusivo para o TRE-SP) | 02 |
| ITEM 10 - SOFTWARE DE GERENCIAMENTO E RELATÓRIO | 08 |
| ITEM 11 - IMPLANTAÇÃO COM HANDS ON | 04 |
| ITEM 12 - TREINAMENTO OFICIAL | 10 |

**LOTE 3 - EXCLUSIVO (TRE-PE): Lote destinado a equipamentos com indicação de marca, exclusivo para o TRE-PE pelas razões expostas neste Termo de Referência.**

| ITENS | QUANTIDADE TRE-PE |
|---|---|
| ITEM 13 - FIREWALL DE BORDA TIPO III | 02 |
| ITEM 14 - FIREWALL DE CARTÓRIO TIPO II | 21 |
| ITEM 15 - SOFTWARE DE GERENCIAMENTO | 01* |
| ITEM 16 - SOLUÇÃO DE ANÁLISE DE LOGS FÍSICA | 02 |
| ITEM 17 - IMPLANTAÇÃO COM HANDS ON | 01 |
| ITEM 18 - TREINAMENTO OFICIAL | 05 |

** A solução de gerenciamento FORTIMANAGER da FORTINET não apresenta licenciamento por unidade, por isso, incluímos o licenciamento mínimo a ser adquirido de uma única vez para os cinco dispositivos necessários.*

**LOTE 4: Lote destinado a equipamentos de porte médio que atenderão aos TRE's que possuem vazão de internet média de 9,1 Gbps, não sendo compatível com nenhum outro lote existente.**

| ITENS | QUANTIDADE TRE-PB | QUANTIDADE TRE-GO | QUANTIDADE TRE-PR | QUANTIDADE TRE-CE | QUANTIDADE TRE-PA | QUANTIDADE TRE-AL | QUANTIDADE TOTAL PARA O LOTE |
|---|---|---|---|---|---|---|---|
| ITEM 19 - FIREWALL DE BORDA TIPO IV | 02 | 04 | 02 | 03 | 02 | 02 | 15 |
| ITEM 20 - FIREWALL DE CARTÓRIO TIPO III | 0 | 70 | 0 | 125 | 00 | 42 | 237 |
| ITEM 21 - SOFTWARE DE GERENCIAMENTO E RELATÓRIO | 02 | 74 | 02 | 128 | 00 | 44 | 250 |
| ITEM 22 - IMPLANTAÇÃO COM HANDS ON | 01 | 02 | 01 | 02 | 01 | 01 | 08 |
| ITEM 23 - TREINAMENTO OFICIAL | 08 | 02 | 06 | 01 | 00 | 04 | 21 |

1.2 - **Farão parte deste Registro de Preços, como órgãos participantes, os Tribunais Regionais Eleitorais – TREs de Alagoas, Amapá, Amazonas, Ceará, Goiás, Pará, Paraíba, Paraná, Rondônia e São Paulo, que serão responsáveis pelas suas respectivas contratações.**

## 2 - FUNDAMENTAÇÃO DA CONTRATAÇÃO

### 2.1 Motivações da Contratação

Em 2021, foram adquiridos pelo TRE-PE firewalls para os cartórios, em licitação aberta a todas as marcas. Nessa licitação, houve a vitória do fabricante FORTINET e acabamos por adquirir 80 equipamentos FORTIGATE 40F para utilização nos cartórios, bem como o software FortiManager usado para gerência e coleta de logs com licenças para todos esses equipamentos adquiridos.

Após essa aquisição, verificamos a dificuldade em trabalhar com marcas diferentes de firewall em um mesmo ambiente, pois já possuíamos os firewalls de borda da marca SonicWall NSA 5600. Com a aquisição dos firewalls de cartório de outra marca, tivemos de dividir o nosso gerenciamento em ambiente não unificado. Além disso, tivemos que prospectar a aquisição de ferramentas e treinamentos específicos para cada uma das marcas. Por outro lado, ainda, a integração entre os equipamentos de diferentes fabricantes não é completa, impedindo o uso de recursos avançados próprios de cada fabricante. Empresas de pesquisa e consultoria em TIC, como a Gartner, indicam que a tendência para o futuro na área de segurança é a padronização das marcas trazendo ganhos em economia e eficiência (https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-securityand-risk-management-trends-for-2022).

Os seguintes fatores nos levaram a buscar a padronização de nossa rede para o fabricante FORTINET:

a) Manutenção do investimento já realizado na compra de firewalls de cartórios eleitorais, softwares de gerência e treinamentos, pois tanto software como equipamentos ainda permanecem em garantia por mais dois anos, além de que nossa equipe se aperfeiçoou na solução da FORTINET ao longo de 2021;

b) Nossos firewalls de borda da marca SonicWall NSA 5600 vêm apresentando gargalos e problemas de desempenho, por não estarem suportando a ativação de serviços de verificação
(ANTISPAM, ANTIVÍRUS e IPS) no tráfego atual de nossa rede de comunicação de dados;

c) Os registros de log que existem na ferramenta de relatório da marca SonicWall não atendem aos logs solicitados nos protocolos de prevenção de incidentes do CNJ e também impedem uma análise mais profunda de ocorrências dentro de nossa rede, visto que alguns registros básicos como, por exemplo, tempo de conexão em uma VPN, não são facilmente deduzidos na solução atual;

d) Com relação ao objetivo estabelecido na ENSEC-PJ, a preservação, a monitoração e a resposta a incidentes de segurança exigem tecnologias que facilitem o gerenciamento de uma grande quantidade de informações históricas (logs);

e) Integração das soluções e melhoria do nível de controle de segurança da informação no TREPE.

Além do investimento realizado em cursos, preparação de equipe e firewalls, reforçamos que manter soluções diferentes de firewall não é adequado, visto que há um maior gasto com ferramentas específicas de gerenciamento de cada marca, descentralização da gerência de equipamentos e ativos, bem como o não aproveitamento de funcionalidades específicas do fabricante. Avaliando o cenário proposto, a equipe de infraestrutura de rede do TRE-PE, formada pela Coordenadoria de Infraestrutura (COINF), pela Seção de Gerenciamento do Núcleo da Infraestrutura (SENIC) e pela Seção de Gerenciamento de Redes de Computadores (SERCO), decidiu, em conjunto, que a melhor opção técnica e estratégica seria pela padronização de equipamentos de firewall e switches no TRE de forma a integrar conhecimento, equipamentos, softwares e funcionalidades do fabricante, bem como aumentar o nível de segurança em nossa rede de dados.

Para possibilitar uma melhor atuação de nossa equipe, que é bem reduzida, os equipamentos a serem adquiridos precisam ser compatíveis com os protocolos das ferramentas disponíveis neste Tribunal, no caso, FortiManager para armazenamento, gerência e coleta de logs, cuja licença foi adquirida em dezembro/2021 (SEI 0015361-04.2021.6.17.8000), e mecanismos de gerenciamento centralizado existentes nos Firewalls Fortinet (FortiLink), também em uso no TREPE.

### 2.1.1 Outros Tribunais

Além dos fatos elencados, fomos selecionados pelo TSE, seguindo a Estratégia Nacional de Cibersegurança para o período de 2021 a 2024 da Justiça Eleitoral, para que fizéssemos a aquisição em conjunto para outros Tribunais, conforme ratificado no SEI 0009733-97.2022.6.17.8000. Tal estratégia tem como objetivo "servir de direcionador para as diversas ações em segurança cibernética necessárias para o ganho de maturidade em capacidade de identificação, proteção, detecção, resposta e recuperação de incidentes de segurança relacionados com a presença das instituições referenciadas no ciberespaço".
A partir da aprovação da referida estratégia em 06 de agosto de 2021, o Grupo de Trabalho em Segurança da Informação, criado pelo TSE, elaborou os seguintes documentos contendo definições estruturantes com relação ao tema cibersegurança:

- A Arquitetura de Cibersegurança, que definiu um rol de soluções tecnológicas para atender à Estratégia de Cibersegurança da Justiça Eleitoral;

- A Estratégia Nacional de Capacitação em Cibersegurança, que definiu as necessidades de capacitação em cibersegurança para o público interno da Justiça Eleitoral, bem como propôs um roteiro de ações de sensibilização, conscientização e capacitação para seus magistrados, servidores e colaboradores.

Definidos os documentos direcionadores, o TSE organizou subgrupos para a realização das ações conjuntas necessárias à consecução dos objetivos definidos, em acordo com os servidores responsáveis pelo tema "cibersegurança" indicados por todos os TREs. Como resultado dessa organização, o TRE-PE, TRE-RO e TRE-AL foram selecionados, sob a coordenação do primeiro, como responsáveis pela aquisição em comento.

Este grupo de trabalho (TRE-PE, TRE-RO e TRE-AL) deverá instruir os artefatos necessários para viabilizar procedimento licitatário e consequente formalização de Ata de Registro de Preços, para que os demais tribunais eleitorais interessados possam adquirir a solução de firewall necessária.

Desde o final de março, já realizamos questionário via Google Forms (Formulário Automatizado RESPOSTA_TRE's (1889866)) para os membros do grupo de CiberSegurança do TSE e tivemos como respostas de TREs interessados na participação os TREs de Rondônia e Alagoas, que também fazem parte do time de contratação, e os TREs de São Paulo, Paraíba e Amazonas.

O TRE-SC respondeu, mas manifestou que não iria querer participar da contratação. Os estudos foram realizados tomando por base inicialmente as necessidades destes Regionais.

A participação dos TREs no certame foi oficializada pelas respostas ao Ofício-Circular 198 (1893530), encaminhado pela Diretoria-Geral do TRE-PE para os outros TREs e TSE. Tais respostas estão presentes no SEI n.º 0016121-16.2022.6.17.8000, e confirmam ou não a participação dos Regionais em nosso processo.

## 2.2 Objetivos da Contratação

I) A solução deverá atender os seguintes requisitos iniciais:

a. Atender os novos requisitos da ENSEC-JUD, não atendidos com o firewall existente no TRE-PE, quais sejam:

*"5.4 Implantar ferramentas de gerência de configuração de sistemas que automaticamente imponham e reapliquem opções de configuração sobre os sistemas em intervalos regulares agendados;*

*6.3 Habilitar o log dos sistemas de forma a incluir informações detalhadas, tais como origem do evento, data, usuário, horário, endereços de origem, endereços de destino e outros elementos úteis;*

*6.6 Implantar Security Information and Event Management (SIEM) ou ferramenta analítica de logs para correlação e análise de logs;*

*6.7 Em uma base regular, revisar os logs para identificar anomalias ou eventos anormais;*

*6.8 Em uma base regular, ajustar as configurações do SIEM de forma a melhor identificar eventos que requeiram ações e diminuir o ruído proveniente de eventos não importantes."*

b. Atender a necessidade de modernização do parque de segurança de equipamentos dos TREs, diminuindo os riscos de possíveis ataques e melhorando a qualidade dos arquivos de registro (logs) das atividades realizadas na rede, facilitando a rastreabilidade e a identificação de incidentes;

c. Mitigar riscos de indisponibilidade dos sistemas com a adoção de equipamento mais atualizado;

d. Melhorar os relatórios gerados de segurança para futuras auditorias operacionais;

e. Melhorar rendimento e escala com a inclusão de novo equipamento com características de processamento e memória bem maiores que o atualmente utilizado, proporcionando uma maior durabilidade da solução na rede do TRE-PE;

f. Atender às solicitações contidas no plano de ação referente à Resolução CNJ n.º 362/2020, relativa ao protocolo de investigação para ilícitos cibernéticos, quanto à guarda de logs e registros.

f.1 Além disso a solução deverá possuir as seguintes características:

- Integração dos recursos de segurança de proteção contra ameaças em um único dispositivo de segurança de rede de alto desempenho;
- Possuir unidade de processamento de segurança (SPU);
- Permitir visibilidade total dos usuários, dispositivos, aplicativos em toda a superfície de ataque e aplicação consistente da política de segurança, independentemente da localização do ativo;
- Proteger contra vulnerabilidades exploráveis da rede com IPS;
- Bloquear automaticamente ameaças no tráfego descriptografado usando inspeção SSL, incluindo o mais recente padrão TLS 1.3 com cifras obrigatórias;
- Bloquear proativamente os ataques sofisticados recém-descobertos em tempo real com IA e serviços avançados de proteção contra ameaças;
- Possuir segmentação adaptada a qualquer topologia de rede;
- Oferecer defesa em segurança profunda, com inspeção e correção L7 de alto desempenho;
- Possuir interfaces de alta velocidade para permitir flexibilidade de implantação;
- Fornecer acesso seguro à web contra riscos internos e externos, mesmo para tráfego criptografado com alto desempenho;
- Bloquear e controlar o acesso à web com base em usuários ou grupos de usuários nos URLs e domínios;
- Bloquear solicitações de DNS contra domínios maliciosos;
- Fornecer proteção avançada em várias camadas contra ameaças de malware de dia zero entregues pela Web.

g. Atender a estratégia nacional de segurança elaborada pelo TSE para o período 2021-2024, que elegeu o TRE-PE como coordenador da aquisição de firewalls.

## 2.3 Benefícios da Contratação

I) Um dos principais benefícios é o incremento dos recursos de segurança da informação do ecossistema digital dos TREs envolvidos na contratação, atendendo aos seguintes objetivos:

a. Atender os novos requisitos da ENSEC-JUD não atendidos com o firewall existente no TRE-PE quais sejam:

*"5.4 Implantar ferramentas de gerência de configuração de sistemas que automaticamente imponham e reapliquem opções de configuração sobre os sistemas em intervalos regulares agendados.*

*6.3 Habilitar o log dos sistemas de forma a incluir informações detalhadas, tais como origem do evento, data, usuário, horário, endereços de origem, endereços de destino e outros elementos úteis.*

*6.6 Implantar Security Information and Event Management (SIEM) ou ferramenta analítica de logs para correlação e análise de logs.*

*6.7 Em uma base regular, revisar os logs para identificar anomalias ou eventos anormais.*

*6.8 Em uma base regular, ajustar as configurações do SIEM de forma a melhor identificar eventos que requeiram ações e diminuir o ruído proveniente de eventos não importantes."*

b. Atender a necessidade de modernização do parque de segurança de equipamentos do TRE-PE, diminuindo os riscos de possíveis ataques e melhorando a qualidade dos arquivos de registro (logs) das atividades realizadas na rede, facilitando a rastreabilidade e a identificação de incidentes;

c. Mitigar riscos de indisponibilidade dos sistemas com a adoção de equipamento mais atualizado;

d. Melhorar os relatórios gerados de segurança para futuras auditorias operacionais;

e. Melhorar rendimento e escala com a inclusão de novo equipamento com características de processamento e memória bem maiores que o atualmente utilizado, proporcionando uma maior durabilidade da solução na rede do TRE-PE;

f. Atender às solicitações contidas no plano de ação referente à Resolução CNJ n.º 362/2020, relativa ao protocolo de investigação para ilícitos cibernéticos, quanto à guarda de logs e registros;

II) Além disso, realizar a aquisição de forma conjunta a nível nacional seguindo a estratégia de CiberSegurança montada pelo TSE, o que gerará os benefícios de uma compra compartilhada, tais como: redução no tempo de aquisição para os demais TREs participantes, economia de esforços através da redução de processos repetitivos, redução de custos por meio da compra de maiores quantidades (economia de escala), dentre outros.

## 2.4 Relação entre a demanda prevista e a quantidade de bens e/ou serviços contratados

I) As demandas existentes para o TRE-PE são:

| ITENS | QUANTIDADE | JUSTIFICATIVA |
|---|---|---|
| ITEM 13 - FIREWALL DE BORDA TIPO III | 02 | Atualmente, como temos dois Centros de Processamento de Dados, precisamos de dois firewalls de borda da mesma marca e modelo para substituir os atualmente utilizados, os dois trabalhando em redundância física e lógica. |
| ITEM 14 - FIREWALL DE CARTÓRIO TIPO II | 25 | Com relação aos firewalls de cartório, atualmente já utilizamos os firewalls FORTIGATE 40F que possuem throughput adequado para o nosso ambiente. Por conta da padronização já implantada, iremos registrar mais 25 unidades para que possamos substituir, em 2023, os últimos firewalls sonicwall existentes à medida que forem saindo da garantia. |
| ITEM 15 - SOFTWARE DE GERENCIAMENTO | 05 | As cinco licenças correspondem ao quantitativo necessário para a inclusão dos firewalls de borda (dois) e três firewalls de cartório a serem adquiridos no software de gerenciamento do TRE. O número não corresponde ao total de firewalls de cartório pois, em aquisição anterior no TRE-PE, recebemos licenças a mais do que o quantitativo solicitado e que podem ser reaproveitadas para estes equipamentos. |
| ITEM 16 - SOLUÇÃO DE ANÁLISE DE LOGS FÍSICA | 02 | Efetuar o armazenamento de registros de logs das ações efetuadas no ambiente de firewalls, em atendimento às solicitações contidas no plano de ação referente à Resolução CNJ n.º 362/2020, relativa ao protocolo de investigação para ilícitos cibernéticos, quanto à guarda de logs e registros. Estão sendo solicitados dois equipamentos para redundância. |
| ITEM 17 - IMPLANTAÇÃO COM HANDS ON | 01 | Efetuar o repasse inicial da solução de firewall implantada, incluindo as configurações realizadas, senhas iniciais e apresentação ao ambiente. O serviço será executado uma única vez. |
| ITEM 18 - TREINAMENTO OFICIAL | 05 | Treinar a equipe técnica nas soluções adquiridas para os itens 15 e 16 que serão soluções complementares em relação ao ambiente existente. O número de treinamentos corresponde ao número de técnicos alocados na SENIC (2) e SERCO (3) que trabalharão diretamente com a solução. |

II) As demandas existentes para os demais lotes (dos demais TREs) foram colhidas através de resposta ao Ofício-Circular 198 (1893530), encaminhado pela Diretoria-Geral do TRE-PE para os outros TREs e TSE presentes no SEI n.º 0016121-16.2022.6.17.8000.

### 2.5 Natureza do Objeto

O objeto é de natureza comum no mercado e consiste de equipamentos de proteção à rede (firewalls) de núcleo (função de distribuição de tráfego na rede interna), borda (função de proteção do perímetro da rede) e cartório (função de conectar com segurança a rede dos cartórios eleitorais), softwares de gerência e emissão de relatórios, serviços de implantação da solução e treinamento.

## 3. ESPECIFICAÇÃO TÉCNICA

### 3.1 Modelo de Execução e Gestão Contratual

#### 3.1.1 Papéis

**Caberá ao Gestor da Contratação:**

a) Cumprir e fazer cumprir nesta contratação as determinações insertas na Resolução TSE 23.702/2022;

b) Reportar-se à Administração Superior e à Contratada quanto à execução da contratação;

c) Comunicar à Diretoria-Geral o descumprimento de cláusula contratual e instaurar procedimento administrativo para apuração de irregularidade quando devidamente autorizado;

d) Encaminhar à COMAP, quando se tratar de material, o Aceite Definitivo do objeto, baseado no Laudo Técnico emitido pelo Fiscal Técnico;

e) Efetuar o acompanhamento, solicitação e emitir o aceite na nota fiscal correspondente;

f) Encaminhar para a comissão de aceite definitivo (por conta do valor) a nota fiscal do objeto da contratação.

**Caberá ao Fiscal Técnico:**

a) Produzir Laudo Técnico de aceite e encaminhá-lo para o Gestor da Contratação.

**Caberá à Contratada:**

a) Manter durante todo o período de vigência contratual as condições de sua habilitação;

b) Responder aos questionamentos ou esclarecimentos efetuados pelo gestor da contratação no tempo indicado na referida solicitação;

c) Cumprir suas obrigações descritas neste Termo de Referência, bem como os requisitos técnicos indicados no item 4 deste documento;

d) Atender às condições de assistência técnica, previstas neste instrumento, durante o prazo de garantia indicado no tópico 4 deste Termo de Referência, após o aceite definitivo do objeto.

#### 3.1.2 Dinâmica

I) Após o início da vigência da ata de registro de preços, a COINF (Coordenadoria de Infraestrutura/STIC/TRE-PE) ou o responsável pela aquisição em cada TRE solicitará à Coordenadoria de Material e Patrimônio (COMAP) ou ao setor responsável no TRE (no caso de outros tribunais), através de meio eletrônico, o pedido de entrega do quantitativo de itens necessários obedecendo ao mínimo e máximo estipulados neste termo de referência.

II) O acompanhamento do pedido de entrega dos equipamentos (ITENS 1, 2, 3, 7, 8, 9, 13, 14, 16, 19 e 20) será realizado pela unidade responsável em cada TRE. No caso do TRE-PE, será realizado pela COMAP/SA.

III) Após a entrega do(s) equipamento(s) solicitados, a COMAP, ou setor responsável, informará à COINF, no caso do TRE-PE, ou ao gestor da contratação em cada TRE, por mensagem eletrônica, do aceite provisório do objeto e encaminhará o objeto e a respectiva nota fiscal para aceite definitivo.

IV) O recebimento e aceites técnicos, provisório e definitivo, serão realizados conforme descrito no item 3.1.6 deste termo de referência pela equipe de gestão da contratação (gestor do contrato e fiscal técnico).

V) Os itens 4, 5, 6, 10, 11, 12, 15, 17, 18, 21, 22 e 23 serão solicitados e acompanhados pela gestão da contratação em cada TRE.

VI) Após a entrega do(s) serviço(s) solicitados, o fiscal técnico da equipe de contratação em cada TRE, efetuará o aceite provisório do objeto e encaminhará a respectiva nota fiscal para aceite definitivo pelo gestor da contratação, conforme item 3.1.6.

VII) Após o aceite definitivo, o gestor da contratação atestará a nota fiscal e a encaminhará de volta para o setor responsável que procederá aos trâmites institucionais de envio para pagamento.

VIII) Em caso de falhas dentro do período de garantia, deverão ser seguidos os procedimentos de garantia definidos neste termo de referência.

### 3.1.3 Instrumentos Formais

I) A solicitação de fornecimento dos bens e/ou da prestação de serviços será formalizada através de meio eletrônico, conforme registrado no tópico 3.1.2 deste documento.

II) A contratação será formalizada através de instrumento contratual entre as partes.

III) A vigência do contrato será a partir da publicação do seu extrato no diário oficial e terá duração de 60 (sessenta) meses para todos os itens relativos a materiais (FIREWALLS, SOFTWARES e FERRAMENTA DE ANÁLISE DE LOG).

IV) A vigência do contrato para os itens de serviços (IMPLANTAÇÃO E TREINAMENTO) contará a partir da publicação do seu extrato no diário oficial e terá duração de 06 (seis) meses.

### 3.1.4 Acompanhamento

I) A gestão do contrato verificará, durante o período de vigência contratual, o cumprimento dos requisitos descritos no tópico 3 deste Termo de Referência, podendo solicitar a aplicação de sanção em caso de descumprimento.

### 3.1.5 Comunicação

I) A comunicação ocorrerá sempre através de mensagem de correio eletrônico endereçada ao representante da Contratada.

### 3.1.6 Recebimento

### 3.1.6.1 - Para os itens 1, 2, 3, 7, 8, 9, 13, 14, 16, 19 e 20:

### I) Entrega dos equipamentos

a) Os equipamentos deverão ser entregues na unidade responsável pelo recebimento em cada TRE (no caso do TRE-PE na Seção de Almoxarifado), localizada nos locais indicados no ANEXO III - Informações sobre Locais de Entrega e Horários para cada TRE solicitante, de segunda-feira a sexta-feira, no horário estipulado no referido anexo, ou em outro horário previamente agendado com a gestão da contratação, no prazo máximo de 75 (setenta e cinco) dias corridos, contados a partir da publicação do extrato do contrato.

b) Todos os produtos fornecidos deverão ser novos, em linha de produção e de primeiro uso;

c) A entrega deverá ser previamente agendada junto ao Tribunal Regional Eleitoral;

d) Os equipamentos deverão atender rigorosamente a todas as especificações técnicas exigidas, inclusive no tocante a marcas, modelos dos componentes e módulos internos e externos, conforme cotados pela licitante.

e) A unidade responsável pelo recebimento em cada TRE atestará no verso da Nota Fiscal o recebimento provisório dos equipamentos e a encaminhará ao Gestor da Contratação para aceite definitivo.

### II) Aceite dos Equipamentos

Os Equipamentos serão recebidos:

a) provisoriamente pela unidade responsável pelo recebimento em cada TRE, para que seja feita a verificação da conformidade dos mesmos com as especificações.

b) definitivamente, após avaliação e homologação pelo fiscal técnico da Contratação, da seguinte forma:

b.1) O exame para comprovação das características técnicas consistirá em avaliações e testes não-destrutivos, por amostragem, realizados em duas etapas:

- Primeira etapa: inspeção visual de todos os equipamentos entregues;

- Segunda etapa: testes funcionais de configuração e desempenho, em, no mínimo, 10% (dez por cento) e não menos do que 01 (um) dos equipamentos recebidos.

b.1.1) O Fiscal Técnico poderá, a seu critério, executar os testes nos demais equipamentos, dentro de um critério de razoabilidade, podendo chegar a 100% dos quantitativos, mas dentro de um prazo máximo de 10 (dez) dias corridos a partir do recebimento provisório.

b.2) As especificações serão avaliadas também por meio de documentos técnicos que acompanham os equipamentos, informações fornecidas pela Contratada e disponível no sítio do fabricante;

b.3) O fiscal técnico deverá, após a comprovação do perfeito funcionamento dos equipamentos e adequação às especificações técnicas, emitir e assinar o **Laudo de Inspeção Técnica TRE**;

b.4) O produto será rejeitado no caso de incompatibilidade com as especificações previstas na proposta ou quando inadequado à sua utilização;

b.5) O prazo para emissão do **Laudo de Inspeção Técnica TRE** será de até 10 (dez) dias corridos (após o recebimento provisório), quando deverá se manifestar, aceitando ou recusando o item objeto do fornecimento;

b.6) O objeto que estiver em desacordo com as especificações do edital terá seu recebimento recusado, devendo o fornecedor, **dentro do prazo de 20 (vinte) dias corridos** após a comunicação pela contratante, substituir o produto adequadamente, sujeitando-se às sanções previstas no Edital e seus anexos;

b.7) Após a inspeção técnica nos equipamentos e verificando que estes estão em perfeitas condições de funcionamento, o Fiscal Técnico deverá encaminhar o **Laudo de Inspeção Técnica TRE** ao Gestor da Contratação para que seja emitido o aceite definitivo;

b.8) Após o recebimento do Laudo de Inspeção Técnica, o Gestor da Contratação emitirá, em até 5 (cinco) dias corridos o aceite definitivo, que por sua vez será item necessário para a liberação da nota fiscal para pagamento;

b.9) O recebimento definitivo não exime o fornecedor de responder pelos vícios aparentes e ocultos segundo as disposições deste termo e as normas de proteção ao consumidor.

### 3.1.6.2 - Para os itens 4, 10, 15 e 21 (software de gerenciamento/ de gerenciamento e relatório):

a) Após o envio de Nota de Empenho, o Gestor da Contratação encaminhará uma solicitação por mensagem eletrônica, solicitando o envio das referidas licenças adquiridas;

a.2) O prazo de entrega das licenças deve ser de, no máximo, 75 (setenta e cinco) dias corridos;

b) O fiscal técnico realizará o aceite provisório verificando se as licenças correspondem às indicadas na proposta em até 10 (dez) dias corridos, quando deverá se manifestar através de **Laudo de Inspeção Técnica TRE**, aceitando ou recusando o item objeto do fornecimento;

c) O objeto que estiver em desacordo com as especificações do edital terá seu recebimento recusado, devendo o fornecedor, **dentro do prazo de 10 (dez) dias corridos** após a comunicação pela contratante, substituir o produto adequadamente, sujeitando-se às sanções previstas no Edital e seus anexos;

d) Após a inspeção técnica nas licenças e verificando que estas estão em perfeitas condições de funcionamento, o Fiscal Técnico deverá encaminhar o **Laudo de Inspeção Técnica TRE** ao Gestor da Contratação para que seja emitido o aceite definitivo;

e) Após o recebimento do Laudo de Inspeção Técnica, o Gestor da Contratação emitirá, em até 5 (cinco) dias corridos o aceite definitivo, que por sua vez será item necessário para a liberação da nota fiscal para pagamento;

f) O recebimento definitivo não exime o fornecedor de responder pelos vícios aparentes e ocultos segundo as disposições deste termo e as normas de proteção ao consumidor.

### 3.1.6.3 - Para os itens 5, 11, 17 e 22 (implantação com hands on):

a) Após o envio de Nota de Empenho, o Gestor da Contratação encaminhará uma solicitação por mensagem eletrônica, agendando a data reservada para a execução dos serviços de implantação que deve ser finalizado em no máximo 30 (trinta) dias corridos a partir do aceite definitivo dos equipamentos adquiridos;

b) A instalação e configuração compreenderá apenas os firewalls de borda e núcleo, sendo uma unidade deste item aplicada à implantação de **até dois** equipamentos de borda ou **até dois** equipamentos de núcleo visando a implantação de alta disponibilidade;

c) A implantação hands on não será aplicada para os firewalls de cartório;

d) A instalação e configuração compreenderá:

d.1) A realização dos ajustes de hardware e software necessários ao funcionamento dos equipamentos.

d.2) Todas as atualizações de firmware ou qualquer outro software componente da solução, para a versão mais atualizada disponível ou a última compatível com as demais soluções deste lote e considerada estável.

d.3) Habilitação de licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados pela solução.

d.4) Inclusão de políticas de segurança encaminhadas pelo respectivo TRE, preexistentes em seu ambiente, para os novos equipamentos;

e) A CONTRATADA deverá, ao final dos trabalhos, fornecer a entrega da documentação técnica completa da solução referente aos procedimentos de instalação e configuração, bem como fornecer um repasse de no mínimo 10h sobre a solução e as configurações realizadas.

f) Os serviços deverão ser realizados por técnicos credenciados pelo fabricante.

g) O fiscal técnico acompanhará os trabalhos e aprovará a documentação técnica entregue em até 10 (dez) dias corridos através de Laudo de Inspeção Técnica.

h) Após, o fiscal técnico encaminhará para o Gestor da Contratação que realizará o ateste na nota fiscal e encaminhará para pagamento no prazo de até 5 (cinco) dias corridos do recebimento do Lauto de Inspeção Técnica.

### 3.1.6.4 - Para os itens 6, 12, 18 e 23 (treinamento oficial)

a) O fornecimento desse item deverá contemplar vouchers oficiais do fabricante no Treinamento da Solução de Gerenciamento para profissionais da contratante;

b) O voucher deverá ter validade de pelo menos 12 (doze) meses, a partir da entrega e deve ser fornecido em até 20 (vinte) dias corridos após o envio da Nota de Empenho;

c) O treinamento deverá ser realizado de acordo com o calendário de treinamento do fabricante e ministrado em centro oficial de treinamento do mesmo ou remotamente, utilizando tecnologia de ensino a distância em horário comercial;

d) Deverá ser ministrado por profissional devidamente credenciado junto ao fabricante e apto a entregar o respectivo treinamento;

e) O treinamento deverá ter carga horária mínima de 40 (quarenta) horas;

f) Após a conferência do voucher, o Gestor da Contratação solicitará a emissão da nota fiscal para devido atesto e encaminhamento para pagamento.

### 3.1.7 Transferência de Conhecimento

I) A transferência de conhecimento será realizada por meio dos itens de implantação e treinamento existentes em cada lote.

### 3.1.8 Propriedade Intelectual

I) As licenças de softwares, ligadas aos equipamentos, porventura fornecidas, deverão ser cedidas de forma definitiva e sem ônus futuro ao TRE-PE.

## 4. REQUISITOS TÉCNICOS

### Como critérios mínimos para a aquisição temos:

### I) Requisitos gerais comuns para os firewalls (ITENS 1, 2, 3, 7, 8, 9, 13, 14, 19 e 20):

1. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN;

   1.1. Para a implantação da funcionalidade de prevenção contra ameaças de malwares desconhecidos (Zero Day) deve ser utilizada uma solução de Sandbox.

2. Possuir sistema de segurança com aplicação de filtros de pacotes baseados em regras, estados de conexão e inspeção profunda de pacotes;

3. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (shaping);

4. Emitir alertas via correio eletrônico, syslog e traps SNMP;

5. Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do hardware e interfaces WAN e performance do equipamento;

6. Possuir, no mínimo, suporte a SNMP v2 e v3;

7. Deve suportar, no próprio firewall, autenticação de usuários locais e integração com serviços de autenticação de diretório LDAP, Microsoft Active Directory e RADIUS;

8. Suportar e efetuar a captura de pacotes e exportação no formato PCAP;

9. Suportar tags de VLAN;

10. Todas as funcionalidades adquiridas de hardware e software devem operar conforme disposto neste Termo de Referência durante o prazo de garantia dos equipamentos, ou seja, o fornecedor deve garantir a atualização completa das funcionalidades no prazo referido, não sendo permitida a cobrança de quaisquer valores adicionais pelo uso dos hardwares e softwares para esse período. As funcionalidades que não precisem de atualização em base externa de fabricante, tais como identificação de usuários, recursos de rede e VPN, deverão permanecer ativas, mesmo que não sejam atualizadas após o fim do prazo da garantia;

11. O fabricante deverá disponibilizar novas versões de firmwares e softwares da solução durante toda vigência da garantia;

12. O equipamento deve ser fornecido em hardware dedicado tipo appliance com sistema operacional otimizado, do mesmo fabricante, para o uso como firewall corporativo multifuncional.

13. O equipamento deve possuir 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI).

14. Fonte de alimentação com operação automática entre 110 e 220V. Excetuando os firewalls de cartório (itens 3, 14 e 20), todos os demais firewalls devem possuir fonte redundante com a mesma característica;

15. Prover servidor DHCP interno suportando no mínimo um escopo por interface e a funcionalidade de DHCP Relay;

16. Prover mecanismo de conversão de endereços (NAT), de forma a possibilitar que uma rede com endereços reservados acesse a Internet a partir de um único endereço IP e possibilitar também um mapeamento 1-1 de forma a permitir com que servidores internos com endereços reservados sejam acessados externamente através de endereços válidos;

17. Possuir suporte a redes IPv6 e IPv4, para no mínimo as seguintes funcionalidades: VPN IPSec, VPN SSL, DNS, DHCP, SNMP, NAT64, NAT66, Roteamento estático e dinâmico;

18. Possuir o gerenciamento de tráfego de entrada e saída por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida;

19. Implementar os serviços de Provedor VPN baseado no protocolo IPsec, com certificação digital, permitindo aplicar através dos túneis as funcionalidades de Next Generation Firewall (NGFW) exigidas;

20. Todos os equipamentos, produtos, peças ou software ofertados deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não deverão ter previsão de descontinuidade de serviço, suporte ou vida, devendo estar em linha de produção do fabricante e cobertos por contratos de suporte e atualização de versão do fabricante pelo período mínimo de 60 (sessenta) meses;

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

22. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes.

23. O equipamento fornecido deve ser próprio para montagem em rack 19”, incluindo kit para adaptação, se necessário, e cabos de alimentação;

24. Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um link agrupado virtualmente (LAG – Link Aggregation Group);

25. Suportar, no mínimo, os protocolos de roteamento dinâmico OSPF v3 e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based;

26. Deve permitir o envio de logs para sistemas de monitoração externos utilizando o padrão syslog, bem como o envio de forma segura através do protocolo SSL/TLS ou outro protocolo que implemente segurança na transferência dos arquivos;

27. Os firewalls de Borda e Núcleo (Itens 1, 2, 7, 8, 9, 13 e 19) devem possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo;

28. Deve implementar controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos

dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego;

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

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

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

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

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

34. Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

35. Deve possuir a capacidade de reconhecer aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, peer-to-peer, sistemas de mensagem instantânea, assim permitindo criar políticas de roteamento inteligente e balanceamento para essas aplicações, mediante regras preestabelecidas, sendo capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes;

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

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

38. Deve permitir bloquear sessões TCP que utilizarem variações do *three-way handshake*, prevenindo assim possíveis tráfegos maliciosos;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

53. Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional, MS Windows 10, MacOS e Linux e para instalação em dispositivos móveis Android e IOS;

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

55. Deve ser possível através de interface ou console de gerenciamento do equipamento visualizar um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuários específicos incluindo

aplicações e URLs acessadas e permitir a criação de relatórios personalizados ou o envio de informações para solução de relatórios personalizados;

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

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

58. Não será exigido licenciamento adicional para o ITEM 14 - FIREWALL DE CARTÓRIO TIPO II do LOTE 3 das funcionalidades de prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL, apenas o licenciamento de suporte e recursos de VPN.

59. Garantia e Suporte

- Deve possuir garantia do fabricante com validade mínima de 60 (sessenta) meses;
- Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;
- Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição, obedecendo à modalidade NBD (Next Business Day);
- Os chamados poderão ser abertos diretamente com o fabricante ou, excepcionalmente, com centro de suporte autorizado, que represente oficialmente o fabricante da solução em território nacional;
- A empresa contratada deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico ou website ou e-mail;
- A contratada deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana, com sistema de help-desk para abertura de chamados de suporte técnico;
- A equipe técnica da contratante poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema;
- Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;
- A contratada deve indicar, por ocasião do início dos trabalhos, os procedimentos para abertura de suporte técnico;
- As horas de atendimento pelo suporte cumulativo da contratada serão realizadas normalmente em horário comercial, no período compreendido entre 08:00 e 18:00, em dias de semana (segunda à sexta).

60. Os firewalls devem possuir solução de Duplo Fator de Autenticação, com as seguintes características:

- Deve permitir gerar senha de uso único (OTP - One-Time Password) através de aplicativo em dispositivo móvel para uso na autenticação de dois fatores;

- Deve estar licenciada ou inclusa sem custo para dispositivos móveis, compatíveis com as plataformas Android e iOS;

- Não serão aceitas soluções que utilizem SMS ou Email para envio de senha de uso único (OTP - One-Time Password) ou token;

- Deve ser licenciada por unidade de firewall ou Cluster, conforme as quantidades especificadas por lote, descritas na seção: “II) REQUISITOS DE FIREWALL ESPECÍFICOS – (ITENS 1, 2, 3, 7, 8, 9, 13, 14, 19 e 20)”.

61.Os firewalls devem ser entregues com todas as interfaces descritas na seção: “II) REQUISITOS DE FIREWALL ESPECÍFICOS – (ITENS 1, 2, 3, 7, 8, 9, 13, 14, 19 e 20)” licenciadas, ativas e prontas para utilização, inclusive com qualquer hardware adicional (Gbic) necessário à conexão da interface;

62.Quando se tratar de interface de conexão de fibra ótica, devem ser entregues patch cords, com no mínimo 1,5 m, na mesma quantidade das interfaces e compatíveis com os transceptores fornecidos.

## II) REQUISITOS DE FIREWALL ESPECÍFICOS – (ITENS 1, 2, 3, 7, 8, 9, 13, 14, 19 e 20):

(*) A taxa de transferência (throughput) deve ser considerada com utilização de recursos necessários para funções de firewall, reconhecimento e controle de aplicações, prevenção contra ameaças de vírus, spywares e IPS ativos.

(**) Deve ser licenciada por unidade de firewall ou Cluster

REQUISITOS DE DESEMPENHO MÍNIMO ESPECÍFICOS - LOTE 1 - ITEM 1 - FIREWALL DE BORDA TIPO I

| **Especificação mínima** | **Valor** |
|---|---|
| Quantidade de interfaces padrão 1 Gbps 1000Base-T RJ-45 ou 1000Base-T SFP | 8 |
| Quantidade de interfaces padrão 10 Gbps SFP+ | 3 |
| Conexões simultâneas | 900.000 (novecentos mil) |
| Novas conexões por segundo | 22.000 (vinte e dois mil) |
| Clientes VPN SSL simultâneos com solução de 2FA (**) | 500 (quinhentos) |
| Capacidade de usuários VPN SSL simultâneos | 500 (quinhentos) |
| Taxa de transferência throughput (*) | 2.3 Gbps |
| Armazenamento Interno Mínimo (HDD, SSD ou Memória Interna não-volátil) | 128 GB |
| Fonte redundante com seleção de entrada automática para 110/220V | Sim |

REQUISITOS DE DESEMPENHO MÍNIMO ESPECÍFICOS - LOTE 1 - ITEM 2 - FIREWALL DE NÚCLEO TIPO I

| **Especificação mínima** | **Valor** |
|---|---|
| Quantidade de interfaces padrão 1 Gbps 1000Base-T RJ-45 ou 1000Base-T SFP | 8 |
| Quantidade de interfaces padrão 10 Gbps SFP+ | 2 |

| | |
|---|---|
| Conexões simultâneas | 2.000.000(dois milhões) |
| Novas conexões por segundo | 115.000 (cento e quinze mil) |
| Clientes VPN SSL simultâneos com solução de 2FA (**) | 2 |
| Taxa de transferência throughput (*) | 3.6 Gbps |
| Armazenamento Interno Mínimo (HDD, SSD ou Memória Interna não-volátil) | 128 GB |
| Fonte redundante com seleção de entrada automática para 110/220V | Sim |

REQUISITOS DE DESEMPENHO MÍNIMO ESPECÍFICOS - LOTE 1 - ITEM 3 - FIREWALL DE CARTÓRIO TIPO I

| **Especificação mínima** | **Valor** |
|---|---|
| Quantidade de interfaces padrão 1 Gbps 1000Base-T RJ-45 ou 1000Base-T SFP | 5 |
| Conexões simultâneas | 200.000(duzentos mil) |
| Novas conexões por segundo | 6000 (seis mil) |
| Clientes VPN SSL simultâneos com solução de 2FA (**) | 1 |
| Taxa de transferência throughput (*) | 0,34 Gbps |
| Armazenamento Interno Mínimo (HDD, SSD ou Memória Interna não-volátil) | 64 GB |

REQUISITOS DE DESEMPENHO MÍNIMO ESPECÍFICOS - LOTE 2 - ITEM 7 - FIREWALL DE BORDA TIPO II

| **Especificação mínima** | **Valor** |
|---|---|
| Quantidade de interfaces padrão 1 Gbps 1000Base-T RJ-45 ou 1000Base-T SFP | 2 |
| Quantidade de interfaces padrão 10 Gbps SFP+ | 8 |
| Conexões simultâneas | 5.000.000 (cinco milhões) |
| Novas conexões por segundo | 228.000 (duzentos e vinte e oito mil) |
| Clientes VPN SSL simultâneos com solução de 2FA (**) | 6.000 (seis mil) |
| Capacidade mínima de usuários VPN SSL simultâneos | 6.000 (seis mil) |
| Taxa de transferência throughput (*) | 30 Gbps |
| Armazenamento Interno Mínimo (HDD, SSD ou Memória Interna não-volátil) | 480 GB |
| Fonte redundante com seleção de entrada automática para 110/220V | Sim |

REQUISITOS DE DESEMPENHO MÍNIMO ESPECÍFICOS - LOTE 2 - ITEM 8 - FIREWALL DE NÚCLEO TIPO II

| **Especificação mínima** | **Valor** |
|---|---|
| Quantidade de interfaces padrão 1 Gbps 1000Base-T RJ-45 | 2 |

| | |
|---|---|
| ou 1000Base-T SFP | |
| Quantidade de interfaces padrão 10 Gbps SFP+ | 8 |
| Conexões simultâneas | 5.000.000 (cinco milhões) |
| Novas conexões por segundo | 228.000 (duzentos e vinte e oito mil) |
| Clientes VPN SSL simultâneos com solução de 2FA (**) | 2 (dois) |
| Taxa de transferência throughput (*) | 30 Gbps |
| Armazenamento Interno Mínimo (HDD, SSD ou Memória Interna não-volátil) | 480 GB |
| Fonte redundante com seleção de entrada automática para 110/220V | Sim |

REQUISITOS DE DESEMPENHO MÍNIMO ESPECÍFICOS - LOTE 2 - ITEM 9 - FIREWALL DE NÚCLEO TIPO III

| **Especificação mínima** | **Valor** |
|---|---|
| Quantidade de interfaces padrão 1 Gbps 1000Base-T RJ-45 ou 1000Base-T SFP | 2 |
| Quantidade de interfaces padrão 10 Gbps SFP+ | 4 |
| Quantidade de interfaces padrão 40 Gbps QSFP+ ou SFP28 | 2 |
| Conexões simultâneas | 2.500.000 (dois milhões e quinhentos mil) |
| Novas conexões por segundo | 228.000 (duzentos e vinte e oito mil) |
| Clientes VPN SSL simultâneos com solução de 2FA (**) | 2 (dois) |
| Taxa de transferência throughput (*) | 9.5 Gbps |
| Armazenamento Interno Mínimo (HDD, SSD ou Memória Interna não-volátil) | 480 GB |
| Fonte redundante com seleção de entrada automática para 110/220V | Sim |

REQUISITOS DE DESEMPENHO MÍNIMO ESPECÍFICOS - LOTE 3 - ITEM 13 - FIREWALL DE BORDA TIPO III

| **Especificação mínima** | **Valor** |
|---|---|
| Quantidade de interfaces padrão 1 Gbps 1000Base-T RJ-45 ou 1000Base-T SFP | 18 |
| Quantidade de interfaces padrão 10 Gbps SFP+ | 14 |
| Conexões simultâneas | 12.000.000 (doze milhões) |
| Novas conexões por segundo | 750.000(setecentos e cinquenta mil) |
| Clientes VPN SSL simultâneos com solução de 2FA (**) | 500 (quinhentos) |
| Capacidade mínima de usuários VPN SSL simultâneos | 10.000 (dez mil) |
| Taxa de transferência throughput (*) | 9.1 Gbps |
| Armazenamento Interno Mínimo (HDD, SSD ou Memória Interna não-volátil) | 2 TB |
| Fonte redundante com seleção de entrada automática para | Sim |

| | |
|---|---|
| 110/220V | |

REQUISITOS DE DESEMPENHO MÍNIMO ESPECÍFICOS - LOTE 3 - ITEM 14 - FIREWALL DE CARTÓRIO TIPO II

| **Especificação mínima** | **Valor** |
|---|---|
| Quantidade de interfaces padrão 1 Gbps 1000Base-T RJ-45 ou 1000Base-T SFP | 5 |
| Conexões simultâneas | 700.000 (setecentos mil) |
| Novas conexões por segundo | 35.000 (trinta e cinco mil) |
| Clientes VPN SSL simultâneos com solução de 2FA (**) | 1 |
| Capacidade mínima de usuários VPN SSL simultâneos | 200 |
| Taxa de transferência throughput (*) | 600 |
| Wi-fi integrado | 802.11 a/b/g/n/ac |
| Não será exigido licenciamento adicional para as funcionalidades de prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL para o firewall de cartório do lote 3, apenas o licenciamento de suporte, identificação de usuário, controle de aplicações e recursos de VPN. | |

REQUISITOS DE DESEMPENHO MÍNIMO ESPECÍFICOS - LOTE 4 - ITEM 19 - FIREWALL DE BORDA TIPO IV

| **Especificação mínima** | **Valor** |
|---|---|
| Quantidade de interfaces padrão 1 Gbps 1000Base-T RJ-45 ou 1000Base-T SFP | 8 |
| Quantidade de interfaces padrão 10 Gbps SFP+ | 4 |
| Quantidade de interfaces padrão 25 Gbps ou 40 Gbps QSFP+ ou SFP28 | 2 de 40Gbps ou 4 de 25 Gbps |
| Conexões simultâneas | 2.500.000 (dois milhões e quinhentos mil) |
| Novas conexões por segundo | 220.000 (duzentos e vinte mil) |
| Clientes VPN SSL simultâneos com solução de 2FA (**) | 600 (seiscentos) |
| Capacidade mínima de usuários VPN SSL simultâneos | 2.000 (dois mil) |
| Taxa de transferência throughput (*) | 9.1 Gbps |
| Armazenamento Interno Mínimo (HDD, SSD ou Memória Interna não-volátil) | 480 GB |
| Fonte redundante com seleção de entrada automática para 110/220V | Sim |

REQUISITOS DE DESEMPENHO MÍNIMO ESPECÍFICOS - LOTE 4 - ITEM 20 - FIREWALL DE CARTÓRIO TIPO III

| **Especificação mínima** | **Valor** |
|---|---|
| Quantidade de interfaces padrão 1 Gbps 1000Base-T RJ-45 ou 1000Base-T SFP | 5 |
| Conexões simultâneas | 200.000 |

| | |
|---|---|
| | (duzentos mil) |
| Novas conexões por segundo | 14.000 (catorze mil) |
| Clientes VPN SSL simultâneos com solução de 2FA (**) | 2 |
| Capacidade mínima de usuários VPN SSL simultâneos | 20 (vinte) |
| Taxa de transferência throughput (*) | 0.66 Gbps |
| Armazenamento Interno Mínimo (HDD, SSD ou Memória Interna não-volátil) | 64 GB |

## III) REQUISITOS ESPECÍFICOS - SOFTWARE DE GERENCIAMENTO E RELATÓRIO (ITENS 4, 10, 21):

1. Deve prover gestão centralizada de todos os dispositivos do lote para cada TRE participante;

1.1. A solução de cada TRE deve ser independente da fornecida para os demais.

2. Deve estar licenciado, no mínimo, para o quantitativo de licenças solicitadas pelo CONTRATANTE. O item será por unidade licenciada;

3. Deve ser homologado e totalmente compatível com os Firewalls especificados neste Termo de Referência para permitir o gerenciamento centralizado e armazenamento de logs dos mesmos, possuindo escalabilidade para acréscimo de, no mínimo, 154 firewalls para o item 4, 8 para o item 10 e 128 para o item 21;

4. Deve ser do tipo Appliance Físico, Appliance Virtual ou solução de software baseada em máquina virtual (VM). Caso seja entregue em appliance físico ele deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja baseada em Máquina Virtual (VM), a PROPONENTE deverá indicar em sua proposta qual a necessidade de hardware a ser disponibilizada para a respectiva instalação;

5. Caso seja em VM, deve ser compatível com VMware ESX(i);

6. Deve suportar operação em alta disponibilidade (HA) sincronizando as mudanças na base de dados entre as estações de gerência;

7. Na data da proposta, nenhum dos softwares ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

8. Permitir acesso concorrente de administradores;

9. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;

10. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

11. Gerar alertas automáticos via Email;

12. A solução deve gerar alertas automáticos via SNMP;

13. Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora;

14. Caso a solução seja entregue com servidor redundante, as alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante;

15. Deve suportar sincronização do relógio interno via protocolo NTP;

16. Deve registrar as ações efetuadas por quaisquer usuários;

17. Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade, podendo ser disponibilizados na internet;

18. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;

19. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;

20. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

21. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;

22. Permitir criação de regras que fiquem ativas em horário definido;

23. Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência;

24. O servidor de gerência deve ser hospedado em um equipamento independente, não exercendo funções de firewall;

25. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta;

26. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;

27. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados;

28. Deve permitir a criação de objetos e políticas compartilhadas;

29. Deve mostrar os status dos equipamentos de firewalls em alta disponibilidade a partir da solução de gerenciamento centralizado;

30. Deve prover console unificada e centralizada;

31. Deve auxiliar na solução e identificação de ameaças;

32. Deve ser do mesmo fabricante dos demais itens do lote;

33. A solução de gerenciamento centralizado e relatório deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos de firewall gerenciados pela solução, além de consolidar os registros de eventos (logs) e relatórios de todos os equipamentos que compõem a solução de proteção de rede;

34. Deve consolidar logs e relatórios de todos os equipamentos de firewall gerenciados;

35. Suportar um volume mínimo de logs de 20 GB/dia;

36. A solução deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a atualização do software para obter novas funcionalidades e correções de bugs;

37. Caso haja soluções específicas para gerenciamento e relatório, a CONTRATADA deverá prover a quantidade de licenças para ambas as soluções.

## IV) REQUISITOS ESPECÍFICOS - SOFTWARE DE GERENCIAMENTO (ITEM 15):

1. Solução de gerenciamento FORTIMANAGER da FORTINET para, no mínimo, 05 dispositivos;

2. A solução da FORTINET não apresenta licenciamento por unidade, por isso, incluímos o licenciamento mínimo a ser adquirido de uma única vez para os cinco dispositivos necessários.

3. A solução deve possuir suporte pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a atualização do software para obter novas funcionalidades e correções de bugs.

PART NUMBER DE REFERÊNCIA: FMG-VM-10-UG

## V) REQUISITOS ESPECÍFICOS - SOLUÇÃO DE ANÁLISE DE LOGS FÍSICA (ITEM 16):

1. Deve prover console unificada e centralizada;

2. Deve auxiliar na solução e identificação de ameaças;

3. Deve ser uma appliance física;

4. Deve ser do mesmo fabricante dos demais itens do lote;

5. Deve possibilitar o armazenamento e tratamento de logs de, no mínimo, 100 dispositivos.

6. Deve estar licenciada para o total de equipamentos firewall disponíveis para o lote;

7. Deve permitir o envio de eventos no padrão SYSLOG ou CEF;

8. Capacidade mínima para 150 Dispositivos/VDOM;

9. Mínimo de 2 interfaces RJ-45 GE;

10. Mínimo de 4 TB de capacidade de armazenamento útil;

11. A solução deve possuir garantia e suporte pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a atualização do software para obter novas funcionalidades e correções de bugs;

12. A solução deve possuir fonte redundante com entrada automática 110/220V.

PART NUMBER DE REFERÊNCIA: FAZ-300G e FC-10-L03HG-247-02-60

## VI) REQUISITOS ESPECÍFICOS - IMPLANTAÇÃO COM HANDS ON (ITENS 5, 11, 17 e 22):

1. A instalação e configuração compreenderá apenas os firewalls de borda e núcleo, sendo uma unidade deste item aplicada à implantação de **até dois** equipamentos de borda ou **até dois** equipamentos de núcleo visando a implantação de alta disponibilidade;

2. A implantação hands on não será aplicada para os firewalls de cartório;

3. Os serviços de instalação e configuração, compreendem, entre outros, os seguintes procedimentos:

3.1. Análise da topologia e arquitetura da rede, considerando os roteadores, servidores de aplicação e firewall já existentes e instalados;

3.2. Análise do acesso Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

3.3. Análise das regras de Firewall existentes e aplicação à solução ofertada dada a colocação desta na Rede deste parque;

3.4. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

3.5. Apresentação em até 15 dias corridos do plano de implantação com o descritivo de todos os serviços a serem executados e topologia física e lógica a ser implementada;

3.6. A realização dos ajustes de hardware e software necessários ao funcionamento dos equipamentos;

3.7. Aplicação de todas as atualizações de firmware ou qualquer outro software componente da solução, para a versão mais atualizada disponível ou a última compatível com as demais soluções deste lote e considerada estável;

3.8. Configuração do sistema de Firewall, VPN, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com as exigências levantadas com as devidas atualizações necessárias;

3.9. Instalação de Sistema de Gerência Centralizada em Appliance Físico, Appliance Virtual ou solução baseada em VM (máquina virtual), de acordo com a oferta da CONTRATADA. O mesmo será considerado entregue, quando for instalado e configurado, com todas as atualizações, configurações e licenças. Deverão ser adicionados a este todos os firewalls instalados contemplados na solução adquirida, e que deverão ser monitorados e gerenciados por este Sistema de Gerência Centralizada;

3.10. Habilitação das licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados pela solução;

3.11. Inclusão de políticas de segurança encaminhadas pelo respectivo TRE, pré-existentes em seu ambiente, para os novos equipamentos.

4. A CONTRATADA deverá, ao final dos trabalhos, fornecer a entrega da documentação técnica completa da solução referente aos procedimentos de instalação e configuração, bem como fornecer um repasse sobre a solução e as configurações realizadas.

4.1. Deve haver geração de relatório e entrega da documentação da instalação com as configurações efetuadas e as decisões tomadas, diagramas e topologias em formato legível e tecnicamente fundamentado;

4.2. A CONTRATADA deverá ministrar treinamento do tipo “Hands On” sobre a solução de Firewall adquirida, incluindo instalação, configurações aplicadas, troubleshoot, monitoramento e gerenciamento;

4.3. A carga horária mínima será de 10 horas;

4.4. O repasse deverá ter caráter prático e se baseará no sistema Firewall efetivamente instalado na CONTRATANTE;

5. É de responsabilidade da CONTRATADA designar um profissional certificado pelo Fabricante, fornecer todo material audiovisual, didático e, caso necessário, outros equipamentos eletrônicos para a realização dos treinamentos, além de impressos.

6. Todos os demais custos, ônus, obrigações e encargos para o treinamento devem ser arcados pela CONTRATADA.

7. O fiscal técnico acompanhará os trabalhos e aprovará a documentação técnica entregue em até 10 (dez) dias corridos.

## VII) REQUISITOS ESPECÍFICOS - TREINAMENTO (ITENS 6, 12, 18 e 23):

1. A contratada deverá disponibilizar um voucher individual para participação no treinamento oficial do fabricante dos Firewalls ofertado;

2. O treinamento deve ser ministrado abrangendo teoria e prática de configuração e administração de solução de firewall de próxima geração, bem como assuntos teóricos relacionados;

3. Deve conter, no mínimo, a seguinte ementa:

    1. Arquitetura e Plataforma;

    2. Configuração da Solução;

    3. Políticas de Segurança e NAT;

    4. Políticas de segurança baseada em aplicação;

    5. Identificação de Aplicações;

    6. Identificação de Usuário;

    7. Bloqueio de ameaças;

    8. Bloqueio de ameaças desconhecidas;

    9. Bloqueio de ameaças em tráfego criptografado;

    10. Análise das informações de tráfego e ameaças detectadas;

    11. Demais assuntos pertinentes à solução;

4. A duração do treinamento, no total, será de, no mínimo, 20h/aula em horário comercial, podendo ser fornecido um único treinamento com toda a ementa ou um conjunto de treinamentos que atendam a ementa mínima;

5. Deve(m) ser emitido(s) certificado(s) de conclusão cobrindo todo(s) o(s) curso(s) aplicado(s) para cada participante;

6. O treinamento deverá ser ministrado pelo próprio fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais;

7. O treinamento deve estar disponível na modalidade presencial nas instalações do fabricante ou da autorizada ou ministrado de forma remota;

8. O fabricante ou autorizada fornecerá os materiais didáticos para ministrar o curso;

9. Não será necessário considerar na proposta os custos de deslocamento, hospedagem e alimentação dos alunos. Esses custos serão de responsabilidade da Contratante.

## 5. VIGÊNCIA

5.1 - A prestação de serviço deverá possuir vigência de 60 (sessenta) meses com o fornecimento de suporte / garantia de hardware / atualização de softwares para todos os itens, com exceção dos itens 5, 6, 11, 12, 17, 18, 22 e 23, relativos a serviços de implantação e treinamento. Para esses itens, a vigência terá duração de 06 (seis) meses.

## 6. PREÇO UNITÁRIO MÁXIMO ADMITIDO

6.1 - O(s) preço(s) unitário(s) máximo(s) admitido(s) para o(s) item(ns) integrante(s) do(s) lote(s) é/são o(s) constante(s) da tabela abaixo:

| Item | Unidade | Material/Serviço | Descrição (Catmat/Catser) | Quant. Mínima | Quant Máxima | Preço Unitário Máximo Admitido (R$) |
|---|---|---|---|---|---|---|
| **LOTE 1** | | | | | | |
| 01 | Un | FIREWALL DE BORDA TIPO I | 481646 - EQUIPAMENTO DE SEGURANÇA DE REDE TIPO: APPLIANCE APLICAÇÃO: FIREWALL | 01 | 10 | 318.701,21 |
| 02 | Un | *FIREWALL DE NÚCLEO TIPO I* | 481646 - EQUIPAMENTO DE SEGURANÇA DE REDE TIPO: APPLIANCE APLICAÇÃO: FIREWALL | 01 | 06 | 389.198,16 |
| 03 | Un | FIREWALL DE CARTÓRIO TIPO I | 481646 - EQUIPAMENTO DE SEGURANÇA DE REDE TIPO: APPLIANCE APLICAÇÃO: FIREWALL | 01 | 195 | 22.708,91 |
| 04 | Un | SOFTWARE DE GERENCIAMENTO E RELATÓRIO | 27464 - LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA SERVIDOR | 01 | 211 | 4.441,29 |
| 05 | Un | IMPLANTAÇÃO COM HANDS ON | 3840 - TREINAMENTO | 01 | 08 | 74.988,21 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | INFORMÁTICA - SISTEMA/SOFTWARE | | | |
| 06 | Un | TREINAMENTO OFICIAL | 3840 - TREINAMENTO INFORMÁTICA - SISTEMA/SOFTWARE | 01 | 09 | 19.310,48 |
| **LOTE 2** | | | | | | |
| 07 | Un | FIREWALL DE BORDA TIPO II | 481646 - EQUIPAMENTO DE SEGURANÇA DE REDE<br><br>TIPO: APPLIANCE<br><br>APLICAÇÃO: FIREWALL | 01 | 04 | 3.140.809,84 |
| 08 | Un | FIREWALL DE NÚCLEO TIPO II | 481646 - EQUIPAMENTO DE SEGURANÇA DE REDE<br><br>TIPO: APPLIANCE<br><br>APLICAÇÃO: FIREWALL | 01 | 02 | 2.856.042,61 |
| 09 | Un | FIREWALL DE NÚCLEO TIPO III | 481646 - EQUIPAMENTO DE SEGURANÇA DE REDE<br><br>TIPO: APPLIANCE<br><br>APLICAÇÃO: FIREWALL | 01 | 02 | 1.975.321,76 |
| 10 | Un | SOFTWARE DE GERENCIAMENTO E RELATÓRIO | 27464 - LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA SERVIDOR | 01 | 08 | 18.288,73 |
| 11 | Un | IMPLANTAÇÃO COM HANDS ON | 3840 - TREINAMENTO INFORMÁTICA - SISTEMA/SOFTWARE | 01 | 04 | 71.388,21 |
| 12 | Un | TREINAMENTO OFICIAL | 3840 - TREINAMENTO INFORMÁTICA - SISTEMA/SOFTWARE | 01 | 10 | 19.310,48 |
| | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **LOTE 3** | | | | | | |
| 13 | Un | FIREWALL DE BORDA TIPO III | 481646 - EQUIPAMENTO DE SEGURANÇA DE REDE<br><br>TIPO: APPLIANCE<br><br>APLICAÇÃO: FIREWALL | 01 | 02 | 1.353.975,09 |
| 14 | Un | FIREWALL DE CARTÓRIO TIPO II | 481646 - EQUIPAMENTO DE SEGURANÇA DE REDE<br><br>TIPO: APPLIANCE<br><br>APLICAÇÃO: FIREWALL | 01 | 21 | 10.530,28 |
| 15 | Un | SOFTWARE DE GERENCIAMENTO | 27464 - LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA SERVIDOR | 01 | 01 | 63.674,88 |
| 16 | Un | SOLUÇÃO DE ANÁLISE DE LOGS FÍSICA | 481646 - EQUIPAMENTO DE SEGURANÇA DE REDE<br><br>TIPO: APPLIANCE<br><br>APLICAÇÃO: FIREWALL | 01 | 02 | 158.691,77 |
| 17 | Un | IMPLANTAÇÃO COM HANDS ON | 3840 - TREINAMENTO INFORMÁTICA - SISTEMA/SOFTWARE | 01 | 01 | 46.000,00 |
| 18 | | TREINAMENTO OFICIAL | 3840 - TREINAMENTO INFORMÁTICA - SISTEMA/SOFTWARE | 01 | 05 | 23.350,00 |
| **LOTE 4** | | | | | | |
| 19 | Un | FIREWALL DE BORDA TIPO IV | 481646 - EQUIPAMENTO DE SEGURANÇA DE REDE<br><br>TIPO: APPLIANCE<br><br>APLICAÇÃO: | 01 | 15 | 1.584.983,27 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | FIREWALL | | | |
| 20 | Un | FIREWALL DE CARTÓRIO TIPO III | 481646 - EQUIPAMENTO DE SEGURANÇA DE REDE<br><br>TIPO: APPLIANCE<br><br>APLICAÇÃO: FIREWALL | 01 | 237 | 22.410,35 |
| 21 | Un | SOFTWARE DE GERENCIAMENTO E RELATÓRIO | 27464 - LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA SERVIDOR | 01 | 250 | 2.349,42 |
| 22 | Un | IMPLANTAÇÃO COM HANDS ON | 3840 - TREINAMENTO INFORMÁTICA - SISTEMA/SOFTWARE | 01 | 08 | 47.788,62 |
| 23 | Un | TREINAMENTO OFICIAL | 3840 - TREINAMENTO INFORMÁTICA - SISTEMA/SOFTWARE | 01 | 21 | 19.496,12 |

## 7. SANÇÕES

7.1 - Conforme disposto no Edital e na Ata de Registro de Preços.

gov.br
Documento assinado digitalmente
JORGE ALVES BASTOS
Data: 15/03/2023 10:34:04-0300
Verifique em https://validar.iti.gov.br

gov.br
Documento assinado digitalmente
SERGIO AUGUSTO FERREIRA DA SILVA
Data: 13/03/2023 23:14:05-0300
Verifique em https://validar.iti.gov.br