Documentos da fase interna, conforme Lei Estadual 19.581/2018

Índice

Apresentam-se, na sequência, os seguintes documentos da fase interna da licitação:

1) Solicitação de compras e serviços e justificativa;

2) Declaração de existência de dotação orçamentária;

3) Pesquisa de preço;

4) Termo de referência;

5) Parecer Jurídico;

6) Decisão administrativa de autorização do certame.

1) Solicitação de compras e serviços e justificativa

DESPACHO

REFERÊNCIA: 17.129.025-2

Curitiba, 27 de novembro de 2020.

Para: Coordenadoria de Planejamento

Assunto: Solicitação de aquisição de estrutura de Firewalls corporativos.

Prezado coordenador,

1. Instauro o protocolo contendo informações sobre a aquisição de uma estrutura corporativa de Firewall de próxima geração (NGFW) para a Defensoria Pública do Estado do Paraná (DPE-PR).
2. Tratam-se de dois equipamentos do tipo NGFW, a fim de criar uma solução tolerante a falhas que funcione em alta disponibilidade, atenda às necessidades de segurança da informação da DPE-PR e garanta maior segurança da rede a partir de recursos avançados como: inspeção profunda dos pacotes de dados, sistema de prevenção de intrusão (IPS), controle e visibilidade de aplicações, filtro de URLs, controle de acesso e proteção contra ameaças de vírus e malwares.
3. A demanda visa atender as necessidades atuais e futuras de sustentação da infraestrutura tecnológica e de segurança da informação da instituição, resultantes do crescimento de fluxo de dados e a necessidade de acesso externo a sistemas da intranet, como é o caso por exemplo do Solar que está sendo implementado pelo DIF, ferramenta para otimizar o processo de atendimento e tramitação de processos aos assistidos, o OTRS para gerenciar e automatizar todos processos de serviço e suporte ao cliente na área de Informática, dentre outros.
4. O objetivo da solução é prover segurança ativa e proteção a todas as informações trafegadas por todos estes sistemas mencionados em uma rede secundária e totalmente distinta da rede principal da DPE-PR, cuja responsabilidade de proteção e administração é da Celepar.
5. Dito isso, foram incluídos nos autos:
    a) Estudo técnico preliminar, realizado pelo DIF, contendo uma pesquisa aprofundada de equipamentos e acessórios junto a diversos fabricantes que já participaram de licitações públicas. Trata-se de um estudo longo e de alta complexidade, porém importantíssimo para a definição das especificações frente aos cenários de infraestrutura da DPE-PR;

b) Anexo I contendo todas as especificações técnicas dos equipamentos, acessórios, licenças, suporte técnico, garantia e treinamento; e
c) Documento com lista de alguns fornecedores com possibilidade de participação do procedimento licitatório.

Atenciosamente,

_____
RENAN KUSTER DE AZEVEDO
Departamento de Informática

ePROTOCOLO

PROTOCOLO INTEGRADO DO ESTADO
Fls. 3a
Mov. 2

Documento: **DespachoFirewall.pdf.**

Assinado digitalmente por: **Renan Kuster de Azevedo** em 27/11/2020 16:41.

Inserido ao protocolo **17.129.025-2** por: **Renan Kuster de Azevedo** em: 27/11/2020 16:40.

Documento assinado nos termos do art. 18 do Decreto Estadual 5389/2016.

A autenticidade deste documento pode ser validada no endereço: **https://www.eprotocolo.pr.gov.br/spiweb/validarAssinatura** com o código: **fecc05b18ff46ecf9c0cf9cb9ca2622b.**

ESTUDO TÉCNICO PRELIMINAR Curitiba, 16 de Julho de 2020.

1. Introdução

O presente Estudo técnico preliminar (ETP) tem por objetivo demonstrar a viabilidade técnica e econômica para a eventual aquisição de solução de proteção de rede baseada em *appliance* com características de *Next Generation Firewall* (NGFW) com garantia no prazo de 60 meses e treinamento presencial, bem como prover todas as informações necessárias para subsidiar esse respectivo processo licitatório respeitando os princípios de ampla concorrência e isonomia.

2. Fundamentação da Contratação e Justificativa:

O objeto trata-se da aquisição de dois equipamentos do tipo NGFW, a fim de criar uma solução tolerante a falhas que funcione em alta disponibilidade, que atenda às necessidades de segurança da informação da Defensoria Pública do Estado do Paraná (DPPR) e garanta maior segurança da rede a partir de recursos avançados de inspeção profunda dos pacotes de dados, sistema de prevenção de intrusão (IPS), controle e visibilidade de aplicações, filtragem de URLs, controle de acesso e proteção contra ameaças de vírus e *malware*s.

Os usuários da DPPR utilizam os recursos de informática tanto para a execução das atividades-meio (administrativas), bem como para as atividades finalísticas (envolvendo a prestação de assistência jurídica integral e gratuita aos necessitados). Esses serviços são considerados essenciais e alguns até mesmo sigilosos para a execução das atividades institucionais, de tal forma que sua indisponibilidade ou o roubo de determinadas informações por terceiros, produziria impacto direto na Instituição.

Com a premissa da possibilidade de acesso a determinados sistemas internos da Defensoria, inicialmente por servidores e posteriormente também por assistidos, torna-

se primordial a necessidade de contratação de uma solução de segurança que proteja essas informações e reduza os riscos de acessos indevidos.

A contratação de uma solução de *firewall* de próxima geração proporcionará segurança ativa e proteção a todas informações trafegadas na infraestrutura de TI, bem como aos sistemas que estarão hospedados na Zona Desmilitarizada (DMZ). Este será o equipamento responsável pela linha frente da defesa para prover a segurança de informação entre os computadores e dispositivos da instituição com a conexão com rede externa (WAN) e a rede interna (LAN).

A seguir uma lista preliminar dos principais sistemas e serviços que serão disponibilizados aos usuários da DPPR para acesso externo:

Solar

O sistema SOLAR (Solução Avançada em Atendimento de Referência) foi desenvolvido pela Defensoria Pública de Tocantins, e tem como objetivo a otimização dos serviços e maior rapidez no processo de atendimento e tramitação de processos aos assistidos.

De acordo com o corregedor-geral, Natanael Ferreira, “O SOLAR vai gerenciar todo o gabinete do defensor e acompanhar toda questão processual, em tempo real". A plataforma possui confiabilidade nos dados recebidos, bem como melhor uniformização de todos os procedimentos Institucionais relacionados ao atendimento do assistido. Os servidores vão ter acesso direto a agenda dos defensores e assim poderão gerenciar o primeiro atendimento, retorno e audiência do defensor.

A Defensoria Pública do Paraná em parceria com a Defensoria de Tocantins está em processo de adesão desta ferramenta que passará a ser utilizada também em breve na Defensoria do Paraná.

Fonte:http://www.defensoria.rr.def.br/comunica%C3%A7%C3%A3o/noticias/2321-solar-%20sistema-que-agiliza-atendimento-do-assistido-ser%C3%A1-%20implantado-na-dpe

OTRS

OTRS (*Open-source Ticket Request System*), é um sistema de código aberto com a finalidade de fazer o gerenciamento de chamados. O OTRS é utilizado na Defensoria Pública do Paraná e colabora a gerenciar e automatizar todos processos de serviço, suporte ao cliente na área de Informática. O sistema conta com um acesso web em que administradores, agentes e clientes interagem por meio de um portal de acesso. Neste portal os clientes podem solicitar ajuda por exemplo para resolução de problemas em geral de TI e solicitações de acesso. Os chamados geram tickets únicos, e esse número permite um acompanhamento adequado da solicitação, entregando aos usuários informações oportunas e diretas das ações tomadas em relação aos seus pedidos.

Fonte: https://www.opservices.com.br/otrs-service-desk/

Odoo

O Odoo é um software de código aberto com a finalidade de realizar a gestão de projetos e tarefas relacionados a área de Informática no DIF. Nele é possível organizar e ter uma visão clara e eficiente dos projetos, acompanhar prazos, fazer delegações, realizar planejamento de projetos determinando o tempo necessário para a sua realização, e análises com a possibilidade de emissão de relatórios completos sobre as atividades.

Sistema Integrado da Corregedoria (SIC)

É um sistema usados pelos defensores públicos com a finalidade de alimentar os procedimentos realizados por eles dentro de sua área de atuação. Com a implementação do Solar, o sistema do SIC será descontinuado pela DPPR.

3. Relação entre a demanda prevista e a quantidade de cada item

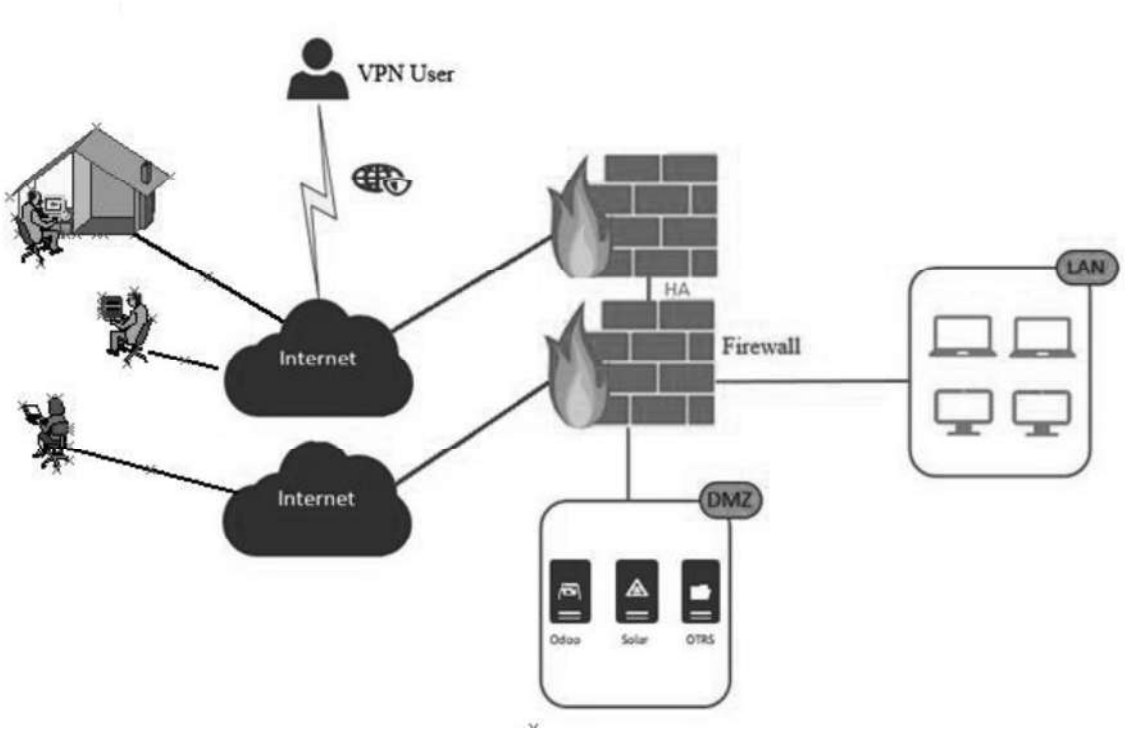
A demanda visa atender as necessidades atuais e futuras de sustentação da infraestrutura tecnológica e de segurança da informação da instituição, resultantes do crescimento de fluxo de dados, necessidades de acesso a sistemas da intranet a partir de uma rede externa e com isso exige-se uma solução de segurança que proteja efetivamente e eleve a segurança desta rede secundária como um todo.

De forma a mensurar esta demanda, levou-se em consideração o levantamento de dois equipamentos do tipo *appliance* de NGFW num cenário de alta disponibilidade podendo funcionar nos modos ativo-passivo ou ativo-ativo, e funcionalidades inteligentes que irão agregar controle de tráfego de dados por identificação de usuários e por camada 7 em referência ao Modelo OSI, com controle de aplicação, filtro URL, administração de largura de banda (QoS), Proteção contra ataques DDoS/DoS, mobilidade a partir de clientes VPN IPsec e SSL, sistema de prevenção de Instrução (IPS), prevenção contra ameaças de vírus e *malware*s, inspeção de tráfego criptografado e balanceamento de carga WAN.

O objeto deste ETP será adjudicado em lote único e composto pelos seguintes itens abaixo:

Item	Demanda prevista	Quantidade
1	*Appliance* de NGFW e licenciamento conforme especificação no Anexo I, por um período mínimo de 5 anos.	2
2	Treinamento da solução ofertada para 5 servidores.	5

4. Cenário prévio da solução:



5. Descrição dos itens da demanda:

Item 1 - Next Generation *Firewall* (NGFW)

Diferentemente de um modelo tradicional de *firewall* que faz controle de tráfego com base apenas em uma política de segurança definida por um conjunto de regras a partir de informações como: IP de origem e IP de destino, porta de origem e porta de destino, tamanho e tipo de serviço, no qual, suas funções limitam-se apenas as Camada 3 (Redes) e Camada 4 (Transporte) em referência ao Modelo OSI o que implica certas limitações, entre elas o não entendimento do que são aplicações, usuários e URLs. O *Firewall* de próxima geração, mais conhecido como NGFW, vai além, com análises mais profundas dos pacotes na camada 7 (Aplicação) que trafegam pela rede com prevenção de invasores e coleta de dados. Também efetua reconhecimento de usuários que possibilita liberação ou bloqueio, roteamento por aplicação e a realização de QoS.

Integrado a este *appliance*, o NGFW pode incluir outros recursos de segurança avançados por meio de subscrição de assinatura, como por exemplo: Sistema de Prevenção de Intrusão (IPS), controle granular e visibilidade de aplicações, controle de filtro de conteúdo web, proteção contra *malware* e VPN.

Licenças:

Para habilitar essas funcionalidades avançadas no *appliance* será necessário adquirir as licenças de cada item. Estas funcionam por meio de subscrição de assinatura, de 1 a 5 anos. A maioria dos fornecedores possuem pacotes com diversas opções de licenças inclusas e isso acaba gerando uma redução de custos a contratante do que se fosse realizado de forma individual.

O vencedor do processo licitatório deverá atender e entregar pelo menos as seguintes licenças abaixo compatíveis com o equipamento ofertado, por um período de subscrição e garantia de 5 anos. O fornecimento é necessário para atender todos os pré-requisitos e manter a proteção e segurança dos dados.

As licenças obrigatórias que deverão estar contidas no item 1 são as seguintes:

- Controle e visibilidade de aplicações

Permite ter visibilidade e controle da rede e realizar políticas de segurança baseada na camada 7 de aplicação onde é possível realizar bloqueios de aplicações como por exemplo: WhatsApp, Facebook e Instagram e também sub-aplicações como por exemplo: Permitir o uso apenas de chat no WhatsApp e Instagram e bloquear funcionalidades de voz e vídeo. Permitir o uso do Facebook para consulta e bloquear jogos, vídeos e streamings da plataforma. O recurso é fundamental para que possamos fazer permissões e bloqueios de forma granular e escalável. Se existir integração com o LDAP é possível criar políticas de controle individuais ou por grupos de usuários.

- Filtro de conteúdo Web

A filtragem de URL fornece o controle granular sobre a atividade de navegação na web com base no que o usuário pode acessar e o que não pode acessar. Basicamente

realiza o controle de filtragem a partir de categorias específicas e listas brancas (permissão), listas negras (bloqueio).

A filtragem de URLs do NGFW é ativada por meio de pesquisas de banco de dados consultando um banco de dados baseado em nuvem do fornecedor da solução.

- Sistema de prevenção de Instrução (IPS)

Diferente do *firewall*, o IPS observa o comportamento do tráfego. É o tipo de inteligência que permite identificar o tráfego e tomar alguma ação de bloqueio para prevenir um ataque malicioso.

- Proteção contra vírus e *malware*

Fornece proteção Gateway Anti-*Malware* e bloqueia todas as formas de vírus, *malware*s, *trojans, keyloggers e spyware* em HTTP e HTTPS, FTP e web e-mails.

- Licenças de Cliente VPN IPSec e SSL

As redes VPN estão baseadas num conceito de tunelamento. Esses túneis exclusivos estabelecem conexões criptografadas para que os dados trafeguem pela rede. Considerando a internet como a infraestrutura, esses pacotes podem são encapsulados por dois tipos de protocolos, IPSEC e SSL.

O IPSec (*Internet Protocol Security*) atua na camada de rede, enquanto o SSL (Secure Sockets Layer) atua na camada de aplicação do Modelo OSI.

A solução fornecida deverá prover as duas modalidades de implementação no equipamento.

IPSec X SSL

IPSec	SSL
Camada 3 (rede) OSI	Camada 7 (aplicação) OSI
Acesso ponto-a-ponto	Acesso remoto
Ideal para conectar filiais	Ideal para conectar usuários. Trabalho remoto

Acess por meio de software	Acesso por meio de portal Web
Suporta qualquer aplicação baseada em IP	Suporta aplicações baseadas na Web e cliente / servidor

- Licença para permitir a Alta disponibilidade (High-Availability - HA)

Permite a possibilidade do *firewall* funcionar na topologia de ativo/ativo e ativo/*standby*. A grande maioria dos fabricantes não cobram valor adicional por essa licença que já está inclusa no equipamento. Caso o fornecedor não possua, será necessário adicioná-la.

- Descriptografia e inspeção de tráfego criptografado.

Descriptografia e inspeção de tráfego TLS/SSL criptografado rapidamente, sem uso de *proxy*, em busca de *malware*, intrusões e vazamento de dados, além de aplicar políticas de controle de aplicações, URL e conteúdo para proteger contra ameaças ocultas no tráfego criptografado. A grande maioria dos fabricantes não cobram valor adicional por essa licença que já está inclusa no equipamento. Caso o fornecedor não possua, será necessário adicioná-la.

- Garantia e suporte das licenças

Permitir contatar o suporte por telefone e baseado na Web pelo menos 8×5: de Segunda a Sexta, das 8h às 17h para ambientes não críticos; Ter acesso direto a ao suporte técnico composto de técnicos/engenheiros para resolução de problemas; Substituição de hardware com troca avançada no caso de falhas; Acessar às documentações e ferramentas oficiais do fabricante do equipamento. Permitir atualização gratuita de firmware do equipamento e licenças em período de vigência de garantia.

Item 2 – Treinamento presencial

O treinamento deve ser oferecido para 5 participantes e ser ministrado por profissional devidamente certificado pelo fabricante da solução ofertada. Este deverá incluir os conhecimentos necessários para a configuração e administração do *appliance* de NGFW e das licenças que serão fornecidas.

6. Demonstrativo de resultados a serem alcançados em termos de economicidade e eficiência.

Um NGFW vai além do que apenas inspecionar tráfegos e realizar bloqueio de portas e protocolos. Esse *appliance* provê mais inteligência e segurança à rede, capaz de impedir a entrada de *malware*, prevenir intrusões, fazer a inspeção profunda dos pacotes a nível de aplicação com controle granular, criar uma política de bloqueio de sites a partir do sistema de filtragem URL, controlar a banda de internet para determinado serviço com QoS e balancear links em casos de *Failover*.

O *Firewall* contribui isolando as máquinas do ambiente externo da Internet, bloqueando acessos que tenham como objetivo explorar vulnerabilidades.

O gerenciamento remoto do equipamento permitirá a possibilidade de execução de atividades de monitoramento, configuração e manutenção sem a necessidade de deslocamento até o local, além disso reduz o tempo entre a identificação do problema e a solução aplicada.

Quanto à garantia contemplada no contrato de 5 anos, permitirá que, durante a vigência, o equipamento esteja sempre atualizado para obter o melhor desempenho e segurança. Em caso de problemas relacionados ao hardware seja realizada a substituição de peças ou de outro equipamento novo pela contratada.

7. Requisitos da Contratação

7.1. Requisitos técnicos

As especificações do objeto desta aquisição encontram-se no **ANEXO I deste Estudo Técnico Preliminar.**

Para um melhor dimensionamento do *appliance* com relação aos pré-requisitos técnicos, o ETP passou pelas seguintes etapas: resposta de questionário técnico de dimensionamento de solução de *firewall* com equipe do DIF, reuniões com especialistas de segurança e pesquisas em sites especializados em segurança e *firewall*.

7.1.1. Questionário - Dimensionamento de *Firewall*

1 - Número de usuários que serão atendidos?
R: Interno: Máx 1000 usuários.
Acesso externo cidadão: +-1000 usuários (futuro)
SIC: 150 users.

2 - Integração com AD/LDAP? Quantas sessões simultâneas?
Poderá existir uma integração.
R: Sim. Máx 1000 usuários. (Será menos, 1000 é um número com margem de segurança)
Total: 1000

3 - Número de interfaces de rede Gigabit ethernet 10/100/1000 (RJ-45).
R: pelo menos 4.

4 - Quantos links WAN e suas capacidades?
R: 1 Link 4Mbps atualmente.
O objetivo é possuir 2 links. O primeiro será aumentado para 100Mbps. E contratação de um segundo link de pelo menos 50Mbps ou 100 Mbps e fazer o balanceamento de carga.

5 - Acesso remoto via SSL VPN ou IPSEC? Quantos usuários simultâneos?
R: Mínimo 20 licenças.

7 - VPN Site-to-Site? Quantas localidades e velocidades dos links?
R: Sem necessidade.

8 - Que tipos de aplicações/serviços passarão por esses links?
R: De forma preliminar os sistemas do Solar, OTRS, SIC, Sistema de almoxarifado, segundo NAS paralelo, Odoo, e outros sistemas que poderão a vir surgir da Defensoria.

9 – Qual é o *Throughput* total (rendimento total) necessário?
Umas das formas de estimar o *Throughput* da rede é somando os links de *download* e *upload* e teremos a taxa de transferência teórica de dados passando pelo *firewall*.

Cálculo:
Link 1 - 100 Mbps (*Download*) + 100 Mbps (*Upload*) = 200 Mbps
Link 2 - 100 Mbps (*Download*) + 100 Mbps (*Upload*) = 200 Mbps
Tráfego Intranet – Aprox 30% - Total: 260 + 260 = 520 Mbps

Com serviços de NGFW habilitados (Controle de aplicações, filtro url, anti-*malware*, ips, vpn) o *appliance* sofre uma degradação de aproximadamente 82% de performance, e mais o serviço de inspeção e Descriptografia de SSL/HTTPS. Sendo assim, é necessário estar atendo as especificações técnicas de *Throughput* de *firewall* e de *Throughput* com todos os serviços habilitados dos fabricantes para evitar qualquer problema.

Recomendação:
Throughput de *firewall*: 3.3 Gbps
Throughput NGFW: 700 Mbps

Fonte:
https://securityboulevard.com/2019/01/next-gen-*firewall*-sizing-5-things-to-look-for/
https://www.*firewall*s.com/blog/*firewall*-tech-specs/

10 - Conexões por segundo (CPS)
O CPS trata da rapidez com que o *firewall* pode criar e armazenar uma nova sessão aceita por uma política de *firewall*.
Estima-se que cada usuário consome de 3 a 7 sessões por segundo para fins de cálculo e dimensionamento seguro.
Cálculo:
2.500 X 7 = 17.500 / Total: 18.000 conexões por segundo.
Fonte:
https://securityboulevard.com/2019/01/next-gen-*firewall*-sizing-5-things-to-look-for/
https://www.*firewall*s.com/blog/*firewall*-tech-specs/

11 - Sessões concorrentes (Tabela máx. *Sessions*)
Refere-se ao número total de sessões de *firewall* que um *appliance* pode suportar.
Estima-se que cada usuário utilize aproximadamente 100 ou mais sessões para fins de cálculo e dimensionamento seguro.
Cálculo:
2500 x 100 = 250.000 + margem de segurança para expansão / Total: 300.000
Fonte:
https://securityboulevard.com/2019/01/next-gen-*firewall*-sizing-5-things-to-look-for/
https://www.*firewall*s.com/blog/*firewall*-tech-specs/

12 - Necessita de alta disponibilidade?
R: Sim. Cenários Ativo/Ativo e Ativo/*Standby*

13 – Necessita de recurso de controle e filtro de URL Web?
R: Sim

14 - Necessita de Controle e visualização de Aplicações?
R: Sim

15 - O equipamento deverá atuar segmentando a rede ou como controle de borda?
R: Controle de borda.

16 – Contrato de garantia e suporte de quanto tempo para o hardware e licenças? Qual a Modalidade pretendida?
R: 60 meses de garantia. 8X5 NBD (Licenças e hardware)

17 - IPS?
R: Sim

18 – Anti-*malware*?
R: Sim

19 - Necessita de inspeção e Descriptografia de tráfego SSL?
R: Sim

20 – Software de gerenciamento? Se sim, em Nuvem?
R: Não necessita.

7.2. Requisitos de negócio

- Sustentação da infraestrutura tecnológica e de segurança da informação.

Aprimorar a segurança da informação com o funcionamento correto dos ambientes de TI combinando tarefas de controle, otimização e segurança para garantir a saúde da rede, sistemas corporativos e dados trafegados.

- Disponibilização de acesso externo a sistemas corporativos:

Permitir acesso da Internet às redes DMZ: somente tipos de tráfego específicos da Internet que são permitidos e são encaminhados às redes DMZ. O *firewall* inspeciona cada sessão e, implicitamente, permite que o tráfego de retorno associado seja encaminhado de volta à Internet.

- VPN de acesso remoto:

Proporcionar aos administradores do DPPR acesso seguro e estável aos recursos de gerenciamento da solução, independentemente de onde o usuário esteja ao se conectar.

- Garantia da disponibilidade de dados:

Permitir através de um cenário de redundância com alta disponibilidade de links e equipamentos podendo estes, operar num cenário ativo/ativo ou ativo/*standby*.

- A solução deve atender à demanda atual e possibilitar o seu uso pelos próximos cinco anos.

- Provimento de treinamento presencial para capacitação técnica da equipe interna:

Capacitar os servidores do DIF sobre a solução de NGFW a respeitos das funcionalidades, configuração e resolução de problemas.

- Provimento de serviços de suporte técnico especializado para a solução de NGFW a ser adquirida no escopo desta contratação:

Contemplar atualizações de *firmware, patchs* e correções de bugs, e suporte técnico presencial (on-site) na modalidade 8x5 NBD.

7.3. Requisitos de capacitação

A empresa contratada deverá transmitir o conhecimento necessário para que os servidores do DIF possam conhecer as características, recursos e funcionalidades da

solução de NGFW ofertada e possa realizar as configurações corretamente de todas as funcionalidades listadas no item 2.1 – Requisitos técnicos.

A capacidade a que se refere, consiste em um treinamento para 5 participantes a ser ministrado por profissional devidamente certificado pelo fabricante da solução ofertada. A infraestrutura para realização do treinamento (eventual locação de sala e laboratório funcional) deverá ser no estado do Paraná e totalmente custeada pela Contratada.

O treinamento deverá incluir os conhecimentos necessários para a configuração, operação e administração dos equipamentos e das licenças. Este deverá ter enfoque prático e ocorrer em "laboratório funcional", ambiente com equipamentos de redes capazes de simular de forma prática aos participantes todos os temas que serão abordados no treinamento (listados abaixo). O material didático deve ser individual, e fornecido pela Contratada (impresso ou em PDF). O conteúdo ministrado pelo instrutor deverá destacar casos práticos em ambientes de produção, e minimizar o conteúdo essencialmente teórico ministrado.

O treinamento deverá ser realizado, em língua portuguesa, possuindo carga horária mínima de 30 (trinta) horas no total, com no máximo 6 (seis) horas diárias, e deverá abordar pelo menos os seguintes temas:

- Visão geral e configuração inicial do equipamento.
- Acessos via GUI, SSH;
- Criação de Políticas de *firewall*.
- Conceitos de zona, objetos, NAT e regras do ambiente.
- Criação de regras de NAT estático e dinâmico;
- Configuração de políticas de *firewall* e recursos de segurança.
- Configuração de DMZ;
- Criação de VLAN's e configuração de VLAN's por Porta, Protocolo, IP Sub-rede;
- IP Routing: Estático e dinâmico;
- Configuração de QoS (*Traffic Shaping e Traffic Policing*);
- Configuração de VPN *site-to-site e client-to-site;*

- VPN IPSec e SSL;
- Autenticação LDAP e integração com o *Microsoft Active Directory*.
- Configuração de HA - Alta Disponibilidade.
- Configuração de recursos de Descriptografia e inspeção de tráfego criptografado
- Conceitos e configuração de cada um dos seguintes recursos: Controle de aplicativos (camada 7); Filtragem de URL; IPS; Proteção contra *malware*.
- Log e alertas.
- Solução de problemas (*Troubleshooting*)

O planejamento das datas e horários deverá ser previamente acordados com o Departamento de Informática da DPPR.

Após a conclusão do treinamento, a Contratada deverá fornecer certificado individual aos participantes dos cursos em até 30 (trinta) dias após sua realização, em língua portuguesa, contendo, no mínimo: instituição, nome do curso, carga horária, nome do treinando, e conteúdo abordado.

7.4. Requisitos de manutenção e garantia

- Suporte e Garantia do fabricante - Quantidade: 60 (sessenta) meses de todos os itens.
- Todos os itens deverão possuir suporte ilimitado para abertura de chamados junto ao Fabricante.
- Atendimento na modalidade 8x5 (NBD – *Next Business Day*) para abertura de chamados: via e-mail, telefone e Internet. Esta deve comprometer-se em manter os registros de todos os chamados constando as descrições dos problemas, e enviar relatório com os chamados por período, sempre que solicitado.
- Em caso de quebra, mau funcionamento, queda de desempenho ou qualquer outro fato causado por defeitos em componentes dos equipamentos, a Contratada deverá providenciar a troca dos componentes por novos, do mesmo modelo ou

tecnicamente superiores, homologados pelo fabricante do equipamento, e deverão ser entregues até o próximo dia útil entre 9 horas e 17 horas (caso o pedido seja recebido antes das 15:00, horário local). Não serão aceitos componentes recondicionados, usados anteriormente ou que possuam desgates aparentes na carcaça ou em algum dos componentes.

- ✓ Caso seja necessário recolher o equipamento para testes em ambiente da contratada, o deslocamento do equipamento será às custas da Contratada. Se houver necessidade de substituição, o Departamento de Informática deverá ser consultado através do e-mail informatica@defensoria.pr.def.br para que indique o procedimento a ser realizado.
- ✓ Os serviços de reparo dos equipamentos especificados serão executados pela contratada/fornecedor na sede Administrativa em Curitiba.
- ✓ Obtenção de imagens e atualizações corretivas de software (firmwares, patches e drivers) do *appliance* de NGFW disponibilizadas pelo fabricante durante o período de garantia.

7.5. Requisitos sociais, ambientais e culturais

Esta contratação busca atender às necessidades da DPPR, obedecendo rigorosamente aos instrumentos legais emitidos pelos órgãos avaliadores de conformidade, tais como a Associação Brasileira de Normas Técnicas – ABNT e o Instituto Nacional de Metrologia, Qualidade e Tecnologia – INMETRO e certificação de Homologação na Anatel.

8. Levantamento de mercado

O mercado oferece diversidade de fabricantes que atendem a esta demanda de segurança da informação.

Com o objetivo de levantar os principais fabricantes de NGFW, a pesquisa teve como fundamento à análise de informações contidas no quadrante mágico do *Gartner* do ano de 2019, a mais atualizada até o momento.

Quadrante mágico do *Gartner*: é um produto da Empresa de consultoria *Gartner Group* criada por *Gideon Gartner* em 1979. O objetivo é criar conhecimento por meio de pesquisas sobre tecnologias, execução de programas, consultoria, eventos e levantamento de soluções para que os usuários (clientes) tomem decisões mais assertivas.

O que é: é representação gráfica do mercado tecnológico por um determinado período. Define forças dentro de um segmento empresarial, fazendo com que fiquem nítidas as qualidades e possíveis falhas das empresas mais significativas da área de tecnologia. Seu objetivo final é funcionar exclusivamente como uma ferramenta de pesquisa para embasar decisões a partir de necessidades específicas de cada negócio.
Ele é dividido da seguinte forma:

1. Líderes (*Leaders*): Aqui são colocadas as empresas tecnologicamente mais avançadas. São aquelas que ditam as regras dentro do seu segmento por ter uma melhor visão de mercado e capacidade de levar adiante as suas promessas.

2. Desafiadores (*Challengers*): São empresas que estão logo atrás dos líderes. São companhias com capacidade de execução plena. Entretanto, apenas possuem uma parcela do mercado.

3. Visionários (*Visionaries*): Nesse ponto temos as empresas mais fortes em pesquisa e desenvolvimento, verdadeiras visionárias. No entanto, muitas vezes não possuem a tecnologia – ou simplesmente não são capazes – para executar o que é prometido.

4. Concorrentes de Nicho (*Nicho Players*): As empresas desse quadrante são aquelas que focam em determinadas características de um mercado.

Figure 1. Magic Quadrant for Network Firewalls

Source: Gartner (September 2019)

Quadrante mágico de solução de *firewall* de rede (Setembro de 2019).

Com base nas informações citadas, o ETP analisou nove fabricantes do mercado:

- Fortinet
- Checkpoint
- Dell Sonicwall
- Barracuda

- Cisco
- Sophos
- Palo Alto
- Forcepoint
- WatchGuard

Para cada fabricante montou-se um quadro comparativo com as principais características e recursos da solução em duas colunas. A primeira corresponde aos pré-requisitos técnicos da Defensoria. E na segunda coluna, dados oficiais do fabricante localizados em documentos técnicos.

Solução 1

Fabricante: Fortinet

Modelo: Fortigate 81F

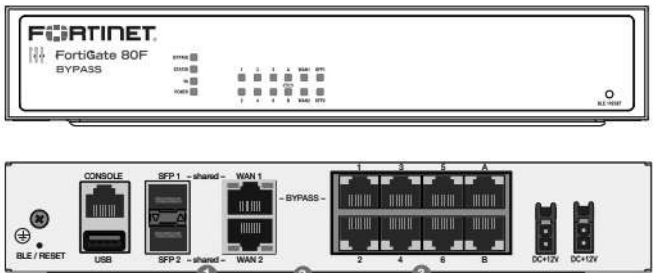


Imagem meramente ilustrativa do modelo Fortigate 81F

	Pré-requisitos	**Fortinet**
		Fortigate 81F
Performance		
Firewall Throughput	3.3 Gbps	10 Gbps
NGFW *Throughput*	700 Mbps	1.0 Gbps
IPS *Throughput*	700 Mbps	1.4 Gbps
Threat Prevention *Throughput*	500 Mbps	250 Mbps
VPN *Throughput*	500 Mbps	6.5 Gbps
New sessions/second	18.000	45.000

Máx. Concurrent sessions	300.000	1.500.000
SSL Inspection	Sim	Sim
NGFW Funcionalidades		
Visibilidade e controle de aplicações	Sim	Sim
Controle e filtro de conteúdo Web	Sim	Sim
IPS	Sim	Sim
Gateway Anti-*malware*	Sim	Sim
Cloud Sandboxing	Opcional	Sim
VPN		
VPN Site-to-site	Não necessário	200
IPSEC VPN Clients	25	2500
SSL-VPN Clients	25	200
Interfaces físicas		
Ethernet interfaces	Pelo menos 5 Interfaces. (5x 1-GbE)	8 x 1-GbE, 2x Shared Media pairs (including 2x GE RJ45 ports, 2x SFP slots), 1x HA port, 1x DMZ port
portas E/S	1 x USB; 1 porta console	1 USB; 1 console (RJ-45)
Alta disponibilidade		
Alta disponibilidade (Ativo/*Standby*)	Modos: Ativo/Ativo e Ativo/*Standby*	Ativo/Ativo, Ativo/*Standby*, Clustering
Failover transparente sem perda de sessão	Necessário	Sim
Detecção de falhas: monitoramento de caminho, monitoramento de interface	Necessário	Sim
Balanceamento de carga	Necessário	Sim
Capacidade de armazenamento		
Storage Module	32 GB SSD	128 GB SSD

Física		
Acompanhar Kit para rack	Necessário	Possui (Opcional)
Fonte	Single	Single AC PS
Forma	Desktop ou rack	Desktop
Funcionalidades de Redes		
Autenticação	AD/LDAP	AD/LDAP
Suporte a NAT	Necessário	Sim
Suporte a VLANs	Necessário	Sim
Roteamento estático	Necessário	Sim
Roteamento dinâmico	Necessário	OSPFv2 and v3, BGP, RIP
Suporte a roteamento IPV4 e IPV6	Necessário	Sim
Controller Wireless no *appliance*		
Wifi controller Integrada; Nº de Aps suportados	Não necessário	Sim; Suporte para até 32 Forti Aps

Licenciamento Fortinet:

A Fortinet possui 4 modalidades de licenciamento. A que melhor se encaixa e atende a todos os pré-requisitos é a licença *Unified Threat Protection* conforme imagem abaixo.

Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Threat Protection
FortiCare	ASE [1]	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard Industrial Service	•	•		
FortiGuard IoT Detection Service [2]	•	•		
FortiConverter Service	•	•		
IPAM Cloud [2]	•			
SD-WAN Orchestrator Entitlement [2]	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.4

Imagem comparativa dos diferentes tipos de licenças do fabricante Fortinet.

Solução 2

Fabricante: Checkpoint

Modelo: 3600

Imagem meramente ilustrativa do modelo Checkpoint 3600

	Pré-requisitos	**Checkpoint**
		3600
Performance		
Firewall Throughput	3.3 Gbps	3.3 Gbps
NGFW *Throughput*	700 Mbps	1.5 Gbps
IPS *Throughput*	700 Mbps	1.99 Gbps
Threat Prevention *Throughput*	500 Mbps	780 Mbps
VPN *Throughput*	500 Mbps	2.71 Gbps
New sessions/second	18.000	32.000
Máx. Concurrent sessions	300.000	2.000.000
SSL Inspection	Sim	Sim
NGFW Funcionalidades		
Visibilidade e controle de aplicações	Sim	Sim
Controle e filtro de conteúdo Web	Sim	Sim
IPS	Sim	Sim
Gateway Anti-*malware*	Sim	Sim
Cloud Sandboxing	Opcional	Sim
VPN		
VPN Site-to-site	Não necessário	Sem informação
IPSEC VPN Clients	25	Sem informação

SSL-VPN Clients	25	Sem informação
Interfaces físicas		
Ethernet interfaces	Pelo menos 5 Interfaces. (5x 1-GbE)	12 x 1-GbE
portas E/S	1 x USB; 1 porta console	2x USB 3.0; 1x Management 10/100/1000 Base-T port; 1x Console (RJ-45); 1x Console (USB Type-C)
Alta disponibilidade		
Alta disponibilidade (Ativo/*Standby*)	Modos: Ativo/Ativo e Ativo/*Standby*	Active/Active L2, Active/Passive L2 and L3
Failover transparente sem perda de sessão	Necessário	Sim
Detecção de falhas: monitoramento de caminho, monitoramento de interface	Necessário	Sim
Balanceamento de carga	Necessário	Sim
Capacidade de armazenamento		
Storage Module	32 GB SSD	8GB. Possibilidade de adicionar 240GB SSD
Física		
Acompanhar Kit para rack	Necessário	Possui (Opcional)
Fonte	Single	Single AC PS, com possibilidade de adição de fonte externa redundante
Forma	Desktop ou rack	Desktop
Funcionalidades de Redes		
Autenticação	AD/LDAP	AD/LDAP
Suporte a NAT	Necessário	Sim

Suporte a VLANs	Necessário	Sim
Roteamento estático	Necessário	Sim
Roteamento dinâmico	Necessário	OSPFv2 and v3, BGP, RIP
Suporte a roteamento IPV4 e IPV6	Necessário	Sim
Controller Wireless no *appliance*		
Wifi controller Integrada; Nº de Aps suportados	Não necessário	Sem suporte

Licenciamento Checkpoint:

A Checkpoint possui 3 modalidades de licenciamento. A que melhor se encaixa e atende a todos os pré-requisitos é a licença NGTP conforme imagem abaixo.

COMPREHENSIVE SOFTWARE BUNDLES

Check Point SOFTWARE TECHNOLOGIES LTD

	NGFW	NGTP	NGTP + SandBlast
Security Gateway Feature Sets			
Firewall	✓	✓	✓
Identity Awareness	✓	✓	✓
IPsec VPN	✓	✓	✓
Advanced Networking & Clustering	✓	✓	✓
Mobile Access	✓	✓	✓
IPS	✓	✓	✓
Application Control	✓	✓	✓
Content Awareness	✓	✓	✓
URL Filtering	o	✓	✓
Antivirus	o	✓	✓
Anti-Spam	o	✓	✓
Anti-Bot	o	✓	✓
SandBlast Threat Emulation	o	o	✓
SandBlast Threat Extraction	o	o	✓
DLP	o	o	o
Security Management Feature Sets			
Network Policy Management	✓	✓	✓
Logging & Status	✓	✓	✓

Imagem comparativa dos diferentes tipos de licenças do fabricante Checkpoint.

Solução 3

Fabricante: Dell Sonicwall

Modelo: NSA 4650

Imagem meramente ilustrativa do modelo Dell Sonicwall NSA 4650

	Pré-requisitos	**Dell Sonicwall** *NSA 4650*
Performance		
Firewall Throughput	3.3 Gbps	6.0 Gbps
NGFW *Throughput*	700 Mbps	Sem informação
IPS *Throughput*	700 Mbps	2.3 Gbps
Threat Prevention *Throughput*	500 Mbps	2.5 Gbps
VPN *Throughput*	500 Mbps	1.45 Gbps
New sessions/second	18.000	40.000
Máx. Concurrent sessions	300.000	3.000.000
SSL Inspection	Sim	Sim
NGFW Funcionalidades		
Visibilidade e controle de aplicações	Sim	Sim
Controle e filtro de conteúdo Web	Sim	Sim
IPS	Sim	Sim
Gateway Anti-*malware*	Sim	Sim
Cloud Sandboxing	Opcional	Sim
VPN		
VPN Site-to-site	Não necessário	1000
IPSEC VPN Clients	25	50(1000)
SSL-VPN Clients	25	2(350)
Interfaces físicas		
Ethernet interfaces	Pelo menos 5 Interfaces. (5x 1-GbE)	4 x 2.5-GbE SFP, 4 x 2.5-GbE, 16 x 1-GbE, 2 x 10GbE SFP+

portas E/S	1 x USB; 1 porta console	2x USB 3.0; 1x Management 10/100/1000 Base-T port; 1x Console (RJ-45);
Alta disponibilidade		
Alta disponibilidade (Ativo/*Standby*)	Modos: Ativo/Ativo e Ativo/*Standby*	Ativo/Ativo, Ativo/*Standby*
Failover transparente sem perda de sessão	Necessário	Sim
Detecção de falhas: monitoramento de caminho, monitoramento de interface	Necessário	Sim
Balanceamento de carga	Necessário	Sim
Capacidade de armazenamento		
Storage Module	32 GB SSD	32GB SSD
Física		
Acompanhar Kit para rack	Necessário	Sim
Fonte	Single	Single AC PS, com possibilidade de adição de fonte externa redundante
Forma	Desktop ou rack	1RU, 19-in. rack-*mountable*
Funcionalidades de Redes		
Autenticação	AD/LDAP	AD/LDAP
Suporte a NAT	Necessário	Sim
Suporte a VLANs	Necessário	Sim
Roteamento estático	Necessário	Sim
Roteamento dinâmico	Necessário	OSPFv2 and v3, BGP, RIP
Suporte a roteamento IPV4 e IPV6	Necessário	Sim

Controller Wireless no *appliance*		
Wifi controller Integrada; Nº de Aps suportados	Não necessário	Sim; Suporte para até 48 Sonic Points

Licenciamento Dell Sonicwall:

A Sonicwall possui 2 modalidades de licenciamento. A que melhor se encaixa e atende a todos os pré-requisitos é a licença Gateway Security Suite (CGSS) conforme imagem abaixo.

Feature	CGSS	AGSS
Gateway Anti-Virus	Y	Y
Intrusion Prevention	Y	Y
Application Control	Y	Y
Content Filtering	Y	Y
24 x 7 Support	Y	Y
Capture ATP	N	Y

AGSS is an upgrade over Comprehensive Gateway Security Suite (CGSS) that adds multi-engine sandboxing for superior protection.

Imagem comparativa dos diferentes tipos de licenças do fabricante Dell Sonicwall.

Solução 4

Fabricante: Barracuda

Modelo: CloudGen *Firewall* F400 STD

Imagem meramente ilustrativa do modelo Barracuda CloudGen *Firewall* F400 STD

	Pré-requisitos	**Barracuda**
		CloudGen Firewall F400 STD
Performance		

Firewall Throughput	3.3 Gbps	7.1 Gbps
NGFW *Throughput*	700 Mbps	2.2 Gbps
IPS *Throughput*	700 Mbps	2.8 Gbps
Threat Prevention *Throughput*	500 Mbps	2.0 Gbps
VPN *Throughput*	500 Mbps	2.3 Gbps
New sessions/second	18.000	20.000
Máx. Concurrent sessions	300.000	500.000
SSL Inspection	Sim	Sim
NGFW Funcionalidades		
Visibilidade e controle de aplicações	Sim	Sim
Controle e filtro de conteúdo Web	Sim	Sim
IPS	Sim	Sim
Gateway Anti-*malware*	Sim	Sim
Cloud Sandboxing	Opcional	Sim
VPN		
VPN Site-to-site	Não necessário	Ilimitado
IPSEC VPN Clients	25	Ilimitado
SSL-VPN Clients	25	Ilimitado
Interfaces físicas		
Ethernet interfaces	Pelo menos 5 Interfaces. (5x 1-GbE)	8 x 1-GbE
portas E/S	1 x USB; 1 porta console	2x USB 2.0, 1x Console (RJ-45)
Alta disponibilidade		
Alta disponibilidade (Ativo/*Standby*)	Modos: Ativo/Ativo e Ativo/*Standby*	Active-passive ; Transparent *failover* without session loss ; Encrypted HA communication
Failover transparente sem perda de sessão	Necessário	Sim

Detecção de falhas: monitoramento de caminho, monitoramento de interface	Necessário	Sim
Balanceamento de carga	Necessário	Sim
Capacidade de armazenamento		
Storage Module	32 GB SSD	SSD 80GB ou mais
Física		
Acompanhar Kit para rack	Necessário	Sim
Fonte	Single	Single AC PS
Forma	Desktop ou rack	1RU, 19-in. rack-*mountable*
Funcionalidades de Redes		
Autenticação	AD/LDAP	AD/LDAP
Suporte a NAT	Necessário	Sim
Suporte a VLANs	Necessário	Sim
Roteamento estático	Necessário	Sim
Roteamento dinâmico	Necessário	OSPFv2 and v3, BGP, RIP
Suporte a roteamento IPV4 e IPV6	Necessário	Sim
Controller Wireless no *appliance*		
Wifi controller Integrada; Nº de Aps suportados	Não necessário	Sem suporte

Licenciamento Barracuda:

O licenciamento da Barracuda é um pouco diferente dos demais. Para atender a demanda, é necessário a licença Basic (que contém basicamente todas as funcionalidades NGFW), e uma licença opcional "*Malware protection*" conforme imagem abaixo.

Basic features

	ENTRY AND BRANCH OFFICE / RUGGED	MID-RANGE	HIGH-END
Firewall incl. IPS	✓	✓	✓
Application control	✓	✓	✓
Dynamic routing	✓	✓	✓
Application-based provider selection	✓	✓	✓
SSL interception	✓	✓	✓
SD-WAN	✓	✓	✓
Web filter	✓	✓	✓
Zero-touch deployment	✓	✓	✓
Client-to-site and site-to-site VPN	Unlimited	Unlimited	Unlimited

Optional features

	ENTRY AND BRANCH OFFICE / RUGGED	MID-RANGE	HIGH-END
Firewall Insights	Optional	Optional	Optional
Advanced threat protection	Optional	Optional	Optional
Malware protection	Optional [1]	Optional	Optional
Advanced remote access	Optional [2]	Optional	Optional

Imagem comparativa dos diferentes tipos de licenças do fabricante Barracuda.

Solução 5

Fabricante: Cisco

Modelo: FirePower 1140

Imagem meramente ilustrativa do modelo Cisco FRP-1140

	Pré-requisitos	**Cisco**
		Cisco FPR-1140
Performance		
Firewall Throughput	3.3 Gbps	6.0 Gbps
NGFW *Throughput*	700 Mbps	2.2 Gbps
IPS *Throughput*	700 Mbps	2.2 Gbps
Threat Prevention *Throughput*	500 Mbps	Sem informação
VPN *Throughput*	500 Mbps	300 Mbps
New sessions/second	18.000	100.000
Máx. Concurrent sessions	300.000	400.000

SSL Inspection	Sim	Sim
NGFW Funcionalidades		
Visibilidade e controle de aplicações	Sim	Sim
Controle e filtro de conteúdo Web	Sim	Sim
IPS	Sim	Sim
Gateway Anti-*malware*	Sim	Sim
Cloud Sandboxing	Opcional	Sim
VPN		
VPN Site-to-site	Não necessário	750
IPSEC VPN Clients	25	750
SSL-VPN Clients	25	750
Interfaces físicas		
Ethernet interfaces	Pelo menos 5 Interfaces. (5x 1-GbE)	8 x 1-GbE, 4 x SFP
portas E/S	1 x USB; 1 porta console	1x Management 10/100/1000 Base-T port; 1x Console (RJ-45), 1 x USB 3.0
Alta disponibilidade		
Alta disponibilidade (Ativo/*Standby*)	Modos: Ativo/Ativo e Ativo/*Standby*	Ativo/Ativo, Ativo/*Standby*
Failover transparente sem perda de sessão	Necessário	Sim
Detecção de falhas: monitoramento de caminho, monitoramento de interface	Necessário	Sim
Balanceamento de carga	Necessário	Sim
Capacidade de armazenamento		
Storage Module	32 GB SSD	SSD 200 GB
Física		

Acompanhar Kit para rack	Necessário	Sim
Fonte	Single	Single AC PS
Forma	Desktop ou rack	1RU, 19-in. rack-*mountable*
Funcionalidades de Redes		
Autenticação	AD/LDAP	AD/LDAP
Suporte a NAT	Necessário	Sim
Suporte a VLANs	Necessário	Sim
Roteamento estático	Necessário	Sim
Roteamento dinâmico	Necessário	OSPFv2 and v3, BGP, RIP
Suporte a roteamento IPV4 e IPV6	Necessário	Sim
Controller Wireless no *appliance*		
Wifi controller Integrada; Nº de Aps suportados	Não necessário	Sem suporte

Licenciamento Cisco:

A Cisco, a licença correspondente aos serviços de NGFW é Cisco *Firepower Threat Defense.*

Solução 6

Fabricante: Sophos

Modelo: XG 125

Imagem meramente ilustrativa do modelo Sophos XG 125

	Pré-requisitos	**Sophos** *XG 125*
Performance		
Firewall Throughput	3.3 Gbps	6.5 Gbps
NGFW *Throughput*	700 Mbps	1.1 Gbps
IPS *Throughput*	700 Mbps	1.53 Gbps
Threat Prevention *Throughput*	500 Mbps	700 Mbps
VPN *Throughput*	500 Mbps	700 Mbps
New sessions/second	18.000	35.000
Máx. Concurrent sessions	300.000	6.000.000
SSL Inspection	Sim	Sim
NGFW Funcionalidades		
Visibilidade e controle de aplicações	Sim	Sim
Controle e filtro de conteúdo Web	Sim	Sim
IPS	Sim	Sim
Gateway Anti-*malware*	Sim	Sim
Cloud Sandboxing	Opcional	Sim
VPN		
VPN Site-to-site	Não necessário	Sem informação
IPSEC VPN Clients	25	Sem informação
SSL-VPN Clients	25	Sem informação
Interfaces físicas		
Ethernet interfaces	Pelo menos 5 Interfaces. (5x 1-GbE)	8 x 1-GbE; 1 x SFP
portas E/S	1 x USB; 1 porta console	2 x USB 2.0 1 x Micro-USB 1 x COM (RJ45) 1 x HDMI
Alta disponibilidade		
Alta disponibilidade (Ativo/*Standby*)	Modos: Ativo/Ativo ou Ativo/*Standby*	Ativo/Ativo ou Ativo/*Standby*

Failover transparente sem perda de sessão	Necessário	Sim
Detecção de falhas: monitoramento de caminho, monitoramento de interface	Necessário	Sim
Balanceamento de carga	Necessário	Sim
Capacidade de armazenamento		
Storage Module	32 GB SSD	SSD integrado (sem especificação)
Física		
Acompanhar Kit para rack	Necessário	Opcional
Fonte	Single	Single AC PS, com possibilidade de adição de fonte externa redundante
Forma	Desktop ou rack	Desktop
Funcionalidades de Redes		
Autenticação	AD/LDAP	AD/LDAP
Suporte a NAT	Necessário	Sim
Suporte a VLANs	Necessário	Sim
Roteamento estático	Necessário	Sim
Roteamento dinâmico	Necessário	OSPFv2 and v3, BGP, RIP
Suporte a roteamento IPV4 e IPV6	Necessário	Sim
Controller Wireless no *appliance*		
Wifi controller Integrada; Nº de Aps suportados	Não necessário	Sem suporte

Licenciamento Sophos:

A Sonicwall muitas modalidades de licenciamento. A que melhor se encaixa e atende a todos os pré-requisitos é a licença EnterpriseGuard conforme imagem abaixo.

XG Firewall Features by Subscription Summary

Features (as listed above)		FullGuard Plus (included in TotalProtect Plus)				
			FullGuard (included in TotalProtect)			
		EnterpriseGuard Plus (included in EnterpriseProtect Plus)				
			EnterpriseGuard (included in EnterpriseProtect)			
	Base Firewall	Sandstorm Protection	Network Protection	Web Protection	Email Protection	Web Server Protection
General Management (incl. HA)	●					
Xstream Architecture	●					
Firewall, Networking and Routing	●					
Base Traffic Shaping and Quotas	●					
Secure Wireless	●					
Authentication	●					
Self-Serve User Portal	●					
Base VPN Options	●					
RED Site-to-Site VPN	●					
Sophos Connect VPN Client	●					
Sandstorm Protection		●				
Threat Intelligence Analysis		●				
Intrusion Prevention (IPS)			●			
ATP and Security Heartbeat™			●			
SD-RED Device Management			●			
Clientless VPN			●			
Synchronized Application Control				●		
Web Protection and Control				●		
Application Protection and Control				●		
Cloud Application Visibility				●		
Web and App Traffic Shaping				●		
Email Protection and Control					●	
Email Quarantine Management					●	
Email Encryption and DLP					●	
Web Application Firewall Protection						●
Logging and Reporting	●	●	●	●	●	●
Sophos Central Management	●	●	●	●	●	●

Imagem comparativa dos diferentes tipos de licenças do fabricante Sophos.

Solução 7

Fabricante: Palo Alto

Modelo: PA-3220

Imagem meramente ilustrativa do modelo Palo Alto PA-3220

	Pré-requisitos	Palo Alto
		PA-3220
Performance		

Firewall Throughput	3.3 Gbps	4.3 Gbps
NGFW *Throughput*	700 Mbps	Sem informação
IPS *Throughput*	700 Mbps	Sem informação
Threat Prevention *Throughput*	500 Mbps	2 Gbps
VPN *Throughput*	500 Mbps	Sem informação
New sessions/second	18.000	57.000
Máx. Concurrent sessions	300.000	1.000.000
SSL Inspection	Sim	Sim
NGFW Funcionalidades		
Visibilidade e controle de aplicações	Sim	Sim
Controle e filtro de conteúdo Web	Sim	Sim
IPS	Sim	Sim
Gateway Anti-*malware*	Sim	Sim
Cloud Sandboxing	Opcional	Sim
VPN		
VPN Site-to-site	Não necessário	Sem informação
IPSEC VPN Clients	25	1024
SSL-VPN Clients	25	200
Interfaces físicas		
Ethernet interfaces	Pelo menos 5 Interfaces. (5x 1-GbE)	12 x 1-GbE; 4x SFP; 4X SFP+
portas E/S	1 x USB; 1 porta console	1X porta de gerenciamento fora de banda 10/100/1000, 2x 10/100/1000 de alta disponibilidade, 1x 10G SFP+ de alta disponibilidade, 1x Porta de console RJ-45, (1) Micro USB
Alta disponibilidade		

Alta disponibilidade (Ativo/*Standby*)	Modos: Ativo/Ativo e Ativo/*Standby*	Ativo/Ativo, Ativo/*Standby*
Failover transparente sem perda de sessão	Necessário	Sim
Detecção de falhas: monitoramento de caminho, monitoramento de interface	Necessário	Sim
Balanceamento de carga	Necessário	Sim
Capacidade de armazenamento		
Storage Module	32 GB SSD	SSD 240 GB
Física		
Acompanhar Kit para rack	Necessário	Sim
Fonte	Single	2 fontes de alimentação
Forma	Desktop ou rack	2U, rack padrão de 19
Funcionalidades de Redes		
Autenticação	AD/LDAP	AD/LDAP
Suporte a NAT	Necessário	Sim
Suporte a VLANs	Necessário	Sim
Roteamento estático	Necessário	Sim
Roteamento dinâmico	Necessário	OSPFv2 and v3, BGP, RIP
Suporte a roteamento IPV4 e IPV6	Necessário	Sim
Controller Wireless no *appliance*		
Wifi controller Integrada; Nº de Aps suportados	Não necessário	Sem suporte

Licenciamento Palo Alto:

A Palo Alto possui o licenciamento separado de cada funcionalidade. É necessário a contratação de várias licenças para atender aos pré-requisitos.

Solução 8

Fabricante: Forcepoint

Modelo: N331

Imagem meramente ilustrativa do modelo Forcepoint N331

	Pré-requisitos	**Forcepoint**
		N331
Performance		
Firewall Throughput	3.3 Gbps	5.0 Gbps
NGFW *Throughput*	700 Mbps	1.0 Gbps
IPS *Throughput*	700 Mbps	350 Mbps
Threat Prevention *Throughput*	500 Mbps	Sem informação
VPN *Throughput*	500 Mbps	2.0 Gbps
New sessions/second	18.000	70.000
Máx. Concurrent sessions	300.000	7.000.000
SSL Inspection	Sim	Sim
NGFW Funcionalidades		
Visibilidade e controle de aplicações	Sim	Sim
Controle e filtro de conteúdo Web	Sim	Sim
IPS	Sim	Sim
Gateway Anti-*malware*	Sim	Sim
Cloud Sandboxing	Opcional	Sim
VPN		
VPN Site-to-site	Não necessário	10.000
IPSEC VPN Clients	25	Sem informação
SSL-VPN Clients	25	Sem informação
Interfaces físicas		

Ethernet interfaces	Pelo menos 5 Interfaces. (5x 1-GbE)	8 x 1-GbE
portas E/S	1 x USB; 1 porta console	3x USB, 1x Console (RJ-45)
Alta disponibilidade		
Alta disponibilidade (Ativo/*Standby*)	Modos: Ativo/Ativo e Ativo/*Standby*	Active-active/active-*standby firewall* clustering up to 16 nodes
Failover transparente sem perda de sessão	Necessário	Sim
Detecção de falhas: monitoramento de caminho, monitoramento de interface	Necessário	Sim
Balanceamento de carga	Necessário	Sim
Capacidade de armazenamento		
Storage Module	32 GB SSD	Sem informação
Física		
Acompanhar Kit para rack	Necessário	Opcional
Fonte	Single	Single AC PS, com possibilidade de adição de fonte externa redundante
Forma	Desktop ou rack	Desktop
Funcionalidades de Redes		
Autenticação	AD/LDAP	AD/LDAP
Suporte a NAT	Necessário	Sim
Suporte a VLANs	Necessário	Sim
Roteamento estático	Necessário	Sim
Roteamento dinâmico	Necessário	OSPFv2 and v3, BGP, RIP
Suporte a roteamento IPV4 e IPV6	Necessário	Sim

Controller Wireless no *appliance*		
Wifi controller Integrada; Nº de Aps suportados	Não necessário	Sem suporte

Licenciamento Forcepoint:

O Modelo da Forcepoint já vem com todas as licenças inclusas no equipamento. A única opcional é a de filtro de URL que deverá ser adiciona para cumprir com os requisitos.

Features	
Anti-Malware (File reputation & AV)	Yes
URL Filtering	Option
Advanced Malware Detection	Option
Web Security Cloud Service Chaining	Yes
IPS Inspection	Yes
Application Control (SSH/SFTP, HTTP, HTTPS, TCP, UDP, TFTP, FTP, DNS)	Yes
Endpoint context	Yes
SD-WAN Multi-Link Optimization	Yes
Server Load Balancing	Yes
Clustering	Yes

Imagem demonstrando as funcionalidades e licenças da Forcepoint.

Solução 9

Fabricante: WatchGuard

Modelo: Firebox M270

Imagem meramente ilustrativa do modelo WatchGuard M270

	Pré-requisitos	**WatchGuard** *Firebox M270*
Performance		
Firewall Throughput	3.3 Gbps	4.9 Gbps
NGFW *Throughput*	700 Mbps	1.6 Gbps
IPS *Throughput*	700 Mbps	2.3 Gbps
Threat Prevention *Throughput*	500 Mbps	2.1 Gbps
VPN *Throughput*	500 Mbps	1.6 Gbps
New sessions/second	18.000	40.000
Máx. Concurrent sessions	300.000	2.000.000
SSL Inspection	Sim	Sim
NGFW Funcionalidades		
Visibilidade e controle de aplicações	Sim	Sim
Controle e filtro de conteúdo Web	Sim	Sim
IPS	Sim	Sim
Gateway Anti-*malware*	Sim	Sim
Cloud Sandboxing	Opcional	Sim
VPN		
VPN Site-to-site	Não necessário	50
IPSEC VPN Clients	25	75
SSL-VPN Clients	25	75
Interfaces físicas		
Ethernet interfaces	Pelo menos 5 Interfaces. (5x 1-GbE)	8 x 1-GbE
portas E/S	1 x USB; 1 porta console	2x USB, 1x Console (RJ-45)
Alta disponibilidade		
Alta disponibilidade (Ativo/*Standby*)	Modos: Ativo/Ativo e Ativo/*Standby*	Ativo/Ativo, Ativo/*Standby*
Failover transparente sem perda de sessão	Necessário	Sim

Detecção de falhas: monitoramento de caminho, monitoramento de interface	Necessário	Sim
Balanceamento de carga	Necessário	Sim
Capacidade de armazenamento		
Storage Module	32 GB SSD	32GB SSD
Física		
Acompanhar Kit para rack	Necessário	Sim
Fonte	Single	Single AC PS
Forma	Desktop ou rack	1RU, 19-in. rack-*mountable*
Funcionalidades de Redes		
Autenticação	AD/LDAP	AD/LDAP
Suporte a NAT	Necessário	Sim
Suporte a VLANs	Necessário	Sim
Roteamento estático	Necessário	Sim
Roteamento dinâmico	Necessário	OSPFv2 and v3, BGP, RIP
Suporte a roteamento IPV4 e IPV6	Necessário	Sim
Controller Wireless no *appliance*		
Wifi controller Integrada; Nº de Aps suportados	Não necessário	Sim; Suporte para até 20 Aps

Licenciamento WatchGuard:

A Sonicwall possui 2 modalidades de licenciamento. A que melhor se encaixa e atende a todos os pré-requisitos é a licença *Basic Security* Suite conforme imagem abaixo.

Imagem comparativa dos diferentes tipos de licenças do fabricante WatchGuard.

9. Estimativas preliminares dos preços.

Para fundamentar o valor estimado, neste estudo utilizou-se de orçamentos enviados por revendas oficiais dos fabricantes.

Foi entrado em contato com todos os nove fabricantes solicitando orçamento e até a data do dia 24/05/2020 foi recebido apenas três propostas conforme tabelas abaixo.

A ausência dos demais orçamentos preliminares neste estudo não constitui lacuna importante uma vez que os processos internos da DPPR determinam a realização de pesquisa de preços com fornecedores antes da autorização para licitar, providência essa que será tomada pelo Departamento de Comprar (DCA) após a elaboração do termo de referência.

Fortinet – Seal Telecom

Data da proposta: 26/08/2020

Fortinet - Seal Telecom - Opção: Suporte de 3 anos			
Part number	Descrição	Quantidade	Valor total
FG-81F	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, 1 pair of LAN bypass, 128GB SSD.	2	R$48.064,76
FC-10-0081F-950-02-36	Unified Threat Protection (UTP) (24x7 FortiCare plus Application Control, IPS, AMP, Web Filtering and Antispam Service) - 3 anos	2	R$74.306,58
Serviço	Serviços de Implantação e Treinamento (25 horas)	1	R$46.930,00
		TOTAL:	**R$169.301,34**

Fortinet - Seal Telecom - Opção: Suporte de 5 anos			
Part number	Descrição	Quantidade	Valor total
FG-81F	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, 1 pair of LAN bypass, 128GB SSD.	2	R$48.064,76
FC-10-0081F-950-02-36	Unified Threat Protection (UTP) (24x7 FortiCare plus Application Control, IPS, AMP, Web Filtering and Antispam Service) - 3 anos	2	R$123.836,12
Serviço	Serviços de Implantação e Treinamento (25 horas)	1	R$46.930,00
		TOTAL:	**R$218.830,88**

Checkpoint – Solo Network

Data da proposta: 04/09/2020

Checkpoint - Solo Network - Opção: Suporte de 3 anos			
Part number	Descrição	Quantidade	Valor total
CPAP-SG36XX-INV	Check Point 3600 *Appliance* - Inventory Unit	2	R$18.144,00
FC-10-0081F-950-02-36	Software Upgrade for 3600 Base *Appliance* with SandBlast subscription package for 1 year	2	R$25.964,80
CPSB-NGTP-3600-2Y	Next Generation Threat Prevention for additional 2 years for 3600 Base *Appliance*	2	R$165.472,00
SN-SER-INFRA-Checkpoint	Treinamento Solução Check Point (30 horas)	1	R$11.000,00
		TOTAL:	**R$220.580,80**

Checkpoint - Solo Network - Opção: Suporte de 5 anos			
Part number	Descrição	Quantidade	Valor total
CPAP-SG36XX-INV	Check Point 3600 *Appliance* - Inventory Unit	2	R$18.144,00
FC-10-0081F-950-02-36	Software Upgrade for 3600 Base *Appliance* with SandBlast subscription package for 1 year	2	R$25.964,80
CPSB-NGTP-3600-2Y	Next Generation Threat Prevention for additional 2 years for 3600 Base *Appliance*	4	R$330.944,00
SN-SER-INFRA-Checkpoint	Treinamento Solução Check Point (30 horas)	1	R$11.000,00
		TOTAL:	**R$386.052,80**

Sophos – Redisul

Data da proposta: 10/09/2020

Sophos - Redisul - Opção: Suporte de 3 anos			
Part number	Descrição	Quantidade	Valor total
XG1CT3HEK	Comutador tipo *firewall* XG 125 Rev.3 (EU/UK/)	2	R$46.514,80
NG1C3CSEA	XG 125 EnterpriseGuard with Enhanced Support - 36 MOS	2	
EN1C3CEAA	XG 125 Enhanced Support - 36 MOS	2	

Redisul	Treinamento - 28 horas - 5 participantes	1	R$9.688,80
		TOTAL:	**R$56.203,60**

10. Escolha e justificativa da solução

É imprescindível que todos os itens ofertados pela Contratada atendam a todos os pré-requisitos da especificação técnica contida no Anexo I deste ETP. Este estudo fundamentou-se em nove fabricantes a partir de informações contidas em seus respectivos documentos oficiais. Todas esses possuem recomendação emitida por entidades de nível internacional responsáveis pela análise de soluções de TIC, como o *Gartner*. Em se tratando dos três orçamentos recebidos, a Redisul enviou uma proposta de NGFW do fabricante Sophos com 36 meses de garantia e comparado com Fortinet e Checkpoint, apresentou um valor aproximadamente quatro vezes menor. Diante dessa questão, e se atender a todos os requisitos técnicos solicitados desde equipamentos, licenças e garantia, o Sophos seria a opção de melhor escolha com uma relação bom de custo benefício mantendo a qualidade e respeitando o princípio da economicidade.

11. Benefícios Esperados

- Aprimorar a gestão de segurança da informação;
- Garantir níveis satisfatórios de segurança da informação no âmbito da TI:
  Os sistemas que serão disponibilizados para acesso externo estarão atrás de uma solução corporativa de NGFW consolidada e que se baseia nas melhores práticas do mercado na área de Segurança da Informação.
- Garantir a efetividade da prestação de serviços de TI;
- Garantir a disponibilidade de serviços: Manter a disponibilidade de sistemas internos da DPPR permitindo o acesso externo a estes por defensores públicos, servidores e assistidos.

- Confiabilidade: Incremento no índice de confiabilidade dos usuários em relação aos serviços/sistemas de infraestrutura de rede, uma vez que este projeto aumentará a segurança, disponibilidade e a performance dos serviços de rede que serão disponibilizados para acesso externo.
- Produtividade: Incremento da produtividade dos usuários através de uma infraestrutura confiável e segura permitindo o acesso a determinados sistemas/serviços de uma rede externa.
- Acesso remoto a partir de cliente VPN: Inicialmente com a finalidade de administrar e gerenciar a solução de segurança a partir de uma rede externa da Defensoria.
- Controle granular e visibilidade de aplicações e filtro URL: Permitir identificar e controlar as aplicações trafegadas pela rede durante os acessos externos dos usuários conectados por VPN. O recurso de filtragem de conteúdo web inibirá que sejam acessados sites e conteúdos inapropriados.
- Prevenção contra invasões e *malware*s: detectar e prevenir a invasão de vírus e *malware*s.
- Aprimorar a governança de TI;
- Aumentar o nível de atendimento e qualidade das operações de serviços de TI;
- Conhecimento Técnico: O uso de um sistema de segurança prevê um conhecimento específico da tecnologia e alguns membros da equipe técnica do Departamento de Informática (DIF) receberão um treinamento da solução ofertada pelo fornecedor vencedor da licitação, que proverá capacidade para gerenciar a solução e dar suporte de primeiro nível, realizar configurações na solução e criar regras e políticas de segurança baseando-se nas melhores práticas, ampliando assim o conhecimento técnico da equipe.

12. Providências para adequação no ambiente da Defensoria.

- ✓ Será necessário que a DPPR faça um upgrade no link de internet atual de 4Mbps para um link de maior capacidade para suprir a necessidade de acessos externos (Recomenda-se 100 Mbps de velocidade).
- ✓ É recomendado a contratação de um segundo link de internet com pelo menos 50Mbps para existir uma redundância de links com a finalidade de manter os serviços sempre disponíveis aos usuários, mesmo diante de queda de um link ou quebra de equipamento, cujo o link migrará de forma transparente e automática para o backup e manterá as conexões, sessões e instâncias já estabelecidas.
- ✓ Espaço físico de pelo menos 2U no rack padrão de 19'' para alocação do switch;
- ✓ Dois pontos elétricos 110V ou 220V.
- ✓ Duas portas livres no switch para conectar à rede.

13. Contratações Públicas Similares

Órgão	Defensoria Pública do Distrito Federal
Pregão eletrônico	Pregão Eletrônico N° 11/2019
Objeto	Contratação de empresa especializada no fornecimento de solução integrada de *Firewall* NEXT GENERATION via subscrições, compreendendo suporte técnico, atualizações e serviços técnicos para o período de 36 (trinta e seis) meses.
Link do edital	http://www.comprasnet.gov.br/consultalicitacoes/download/download_editais_detalhe.asp?coduasg=926314&modprp=5&numprp=112019

Órgão	Tribunal Regional Eleitoral do Paraná
Pregão eletrônico	Pregão Eletrônico N.º 66/2019
Objeto	Registro de Preços para aquisição de solução de proteção de rede com características de Next Generation *Firewall* (NGFW) para segurança de informação perimetral que inclui filtro de pacotes, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e *malware*s "*Zero Day*", Filtro de URL, funcionalidade de Sandbox, bem como controle de transmissão de dados e acesso à Internet, compondo uma plataforma de segurança integrada com garantia e respectiva subscrição por, pelo menos, 36 (trinta e seis) meses, serviços de instalação e treinamento, visando atender às necessidades deste Tribunal Regional Eleitoral.
Link do edital	http://www.comprasnet.gov.br/consultalicitacoes/download/download_editais_detalhe.asp?coduasg=70019&modprp=5&numprp=662019

Órgão	Conselho Regional de Contabilidade de Minas Gerais
Pregão eletrônico	Pregão Eletrônico N.º 481/2019
Objeto	O objeto da presente licitação é a seleção da proposta mais vantajosa para a contratação de empresa especializada em solução de segurança de internet, compondo-se de *Appliance* de *Firewall* da Próxima Geração (NGFW), *Appliance* de monitoramento e armazenamento de Logs, na modalidade de entrega de serviços, incluindo implementação da solução, treinamento e suporte técnico em toda solução, conforme condições e especificações estabelecidas no Anexo I – Termo de Referência deste Edital.

Link do edital	https://www.crcmg.org.br/licitacoes/download-licitacao/pagina/18/educacao/contato/id/7977

Órgão	Conselho Regional de Administração de São Paulo
Pregão eletrônico	Pregão Eletrônico N.º 02/2020
Objeto	A contratação de empresa especializada para o fornecimento de soluções integradas de segurança de dados, composto por UTM (Gerenciamento Unificado de Ameaças) e *Endpoint*. As soluções devem possibilitar a visibilidade e controle de tráfego, filtragem de conteúdo Web, prevenção contra ameaças virtuais, filtro de dados, VPN e controle granular de banda de rede, QOS e outras funcionalidades, conforme descritas neste edital e seus anexos.
Link do edital	http://www.comprasnet.gov.br/consultalicitacoes/download/download_editais_detalhe.asp?coduasg=926535&modprp=5&numprp=22020

Órgão	Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira
Pregão eletrônico	Pregão Eletrônico N.º 03/2020
Objeto	O objeto da presente licitação é a escolha da proposta mais vantajosa para a aquisição de solução de segurança de rede composta de *firewall* corporativo e multifuncional para prover segurança e proteção da rede de computadores, contemplando gerência unificada com garantia de funcionamento, incluindo todos os softwares e suas licenças de uso, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua e suporte técnico durante o período de garantia com repasse de conhecimento

	da solução, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.
Link do edital	http://www.comprasnet.gov.br/consultalicitacoes/download/download_editais_detalhe.asp?coduasg=153978&modprp=5&numprp=32020

14. Estratégia para a contratação

14.1. Justificativa para o parcelamento ou não da solução

O parcelamento não se aplica, uma vez que todos os equipamentos e a garantia a serem fornecidos e prestados, são componentes de uma única solução de TI, a qual não pode ser desmembrada sem que haja perda de compatibilidade entre os itens do mesmo lote, tendo em vista a necessidade de padronização. Cabe ressaltar também que não é viável o parcelamento dos serviços prestados, pois geraria riscos à continuidade da solução, dificultando a gestão e gerenciamento da mesma. É necessário que todos os itens sejam do mesmo fabricante e compatíveis a fim de garantir o perfeito funcionamento.

O item treinamento presencial também não poderá ser desmembrado em função de estar relacionado aos demais itens do mesmo lote, ou seja, depende do fabricante vencedor do lote. Baseia-se na solução que será feita a aquisição.

14.2. Prazo de garantia

Os itens 1 e 2 referentes aos equipamentos da solução de segurança NGFW e licenças, respectivamente, deverão ter garantia oficial do fabricante, por um período mínimo 60 (sessenta) meses.

14.3. Análise de Riscos

Não se aplica. A DPPR ainda não possui uma metodologia de Plano de Tratamento de Riscos estabelecida.

RENAN KUSTER DE AZEVEDO

Departamento de Informática

ePROTOCOLO

PROTOCOLO INTEGRADO DO ESTADO
Fls. 55a
Mov. 3

Documento: **EstudoTecnicoPreliminarFirewall.pdf.**

Assinado digitalmente por: **Renan Kuster de Azevedo** em 27/11/2020 16:42.

Inserido ao protocolo **17.129.025-2** por: **Renan Kuster de Azevedo** em: 27/11/2020 16:41.

Documento assinado nos termos do art. 18 do Decreto Estadual 5389/2016.

A autenticidade deste documento pode ser validada no endereço: **https://www.eprotocolo.pr.gov.br/spiweb/validarAssinatura** com o código: **e933293d2243b0fde893cdee761f5835.**

ANEXO I - Estudo Técnico Preliminar

1. Solução integrada de *Firewall* de próxima geração

1.1. Descrição

1.1.1. Aquisição de Solução de *Firewall* baseada em *appliance* (*hardware* dedicado), incluindo o *hardware* e licenças, com características de *Next Generation Firewall* (NGFW) incluindo recursos de filtro de URL, controle de aplicações, VPN, IPS, proteção contra *malwares* e permita a realização de inspeção SSL, compondo uma plataforma de segurança integrada e robusta de um único fabricante, em cenário de alta disponibilidade, com garantia de 60 meses tanto do *hardware* como das licenças;

1.1.2. Não serão aceitos equipamentos de propósito genérico (PC's ou servidores ou máquinas virtuais) sobre os quais podem instalar e ou executar um sistema operacional regular como "*Microsoft Windows", "FreeBSD", "SUN Solaris", "Apple OS X"* ou "*GNU/Linux*".

1.1.3. Os equipamentos deverão contemplar as seguintes funcionalidades:

1.1.3.1. Next Generation *Firewall*;

1.1.3.2. IPS;

1.1.3.3. Controle de aplicações;

1.1.3.4. Filtro de URL;

1.1.3.5. Proteção contra ameaças;

1.1.3.6. VPN IPSEC e SSL;

1.1.3.7. Inspeção SSL.

1.1.3.8. Alta disponibilidade (HA)

1.1.4. Todas as funcionalidades citadas acima deverão ser providas em um único equipamento.

1.1.5. Os equipamentos (*appliances*) fornecidos para o cenário de Alta disponibilidade devem ser do mesmo fabricante, modelo e configuração.

1.1.6. Na data da proposta, nenhum dos modelos ofertados poderá estar listado no site do fabricante em como *end-of-life* ou *end-of-sale*.

1.1.7. Os equipamentos deverão ser fornecidos com todos os itens acessórios de *hardware*, *firmware* e *softwares* necessários à sua perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, *drivers*, programas de configuração, etc.

1.1.8. Os equipamentos deverão estar acompanhados de sua documentação técnica completa e atualizada, contendo os manuais, guias de instalação e outros pertinentes. A documentação deverá ser fornecida em sua forma original, não sendo aceitas cópias de qualquer tipo.

1.1.9. Todas as características exigidas deverão ser comprovadas, independente da descrição da proposta, por meio de documentos oficiais do fabricante, como catálogos, manuais e fichas de especificação técnica, sob pena, na falta destes, de não aceitação do equipamento ofertado.

1.2. Características de *hardware*:

1.2.1. O equipamento deve ser compatível com *rack* de largura padrão de 19 polegadas, padrão EIA-310, e ocupar no máximo 2U. Todos os acessórios necessários para a montagem no *rack* deverão acompanhar o produto, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.2.2. Possuir fonte de alimentação AC bivolt, com chaveamento automático ou manual (tensão na faixa de 100 a 240 Volts) e frequência (de 50/60Hz);

1.2.3. A Fonte deverá ser interna ao equipamento.

1.2.4. Possuir LEDs de identificação de atividades de status do sistema, de cada porta e de energia.

1.2.5. Possuir, no mínimo, 5 (cinco) interfaces de rede *Gigabit Ethernet* 10/100/1000 Base-TX.

1.2.6. Possuir, no mínimo, 1 (uma) interface de rede 10/100/1000 Gbps dedicada para gerenciamento.

1.2.7. Possuir pelo menos 1 (uma) porta console de conexão para acesso a interface de comando CLI especifica para esta finalidade, utilizando cabo do tipo serial RS-232 ou RJ-45;

1.2.8. Possuir pelo menos 1 (uma) porta do tipo USB 2.0 ou 3.0 (*Universal Serial Bus*).

1.2.9. Possuir um disco interno de no mínimo 32GB, do tipo SSD (*Solid-state drive*).

1.3. Dos Requisitos mínimos de capacidade e performance, deve:

1.3.1. Possuir "*Firewall*" com *throughput* mínimo de 3,3 Gbps para pacotes do tipo "UDP" de tamanho de 1.518 (Mil quinhentos e dezoito) bytes.

1.3.2. Possuir *throughput* mínimo de 700 Mbps de NFGW com as seguintes funcionalidades habilitadas simultaneamente, devidamente ativadas e atuantes: *Firewall*, Controle de aplicação, filtro de URL, IPS e *Anti-malware*.

1.3.3. Possuir *throughput* mínimo de 700 Mbps para tráfego IPS;

1.3.4. Possuir *throughput* mínimo de 500 Mbps para proteção contra vírus e malwares.

1.3.5. Possuir *throughput* mínimo de 500 Mbps para tráfego de VPN.

1.3.6. Suportar no mínimo 50 túneis de "VPN SSL" *"client to site*".

1.3.7. Os appliances devem vir licenciados com 25 licenças de cliente VPN SSL.

1.3.8. Suportar no mínimo 300.000 (trezentos mil) conexões simultâneas;

1.3.9. Suportar no mínimo 18.000 (dezoito mil) novas conexões por segundo;

1.3.10. Possuir a funcionalidade de balanceamento e contingência de links;

1.3.11. Deve ser capaz de operar em alta disponibilidade (HA) nos modos de redundância Ativo/Passivo ou Ativo/Ativo com divisão de cargas.

1.3.12. A licença de alta disponibilidade (HA) deve estar inclusa na solução e ser fornecida pela contratada.

1.3.13. Deve suportar cluster do tipo *Failover* (HA) com replicação da tabela de estado para que não haja perda de conexões em caso de falha;

1.3.14. O HA (modo de Alta-Disponibilidade) deve possibilitar a monitoração de falhas dos links.

1.3.15. A comprovação dos requisitos de capacidade e performance deve ser realizada com base em documentação oficial do fabricante da solução ofertada.

1.4. Das funcionalidades de *firewall*, deve:

1.4.1. Possuir tecnologia de *firewall* do tipo *Stateful*;

1.4.2. Deve permitir acesso à internet de forma segura e com registro de toda a atividade de entrada e saída de informações;

1.4.3. Deve suportar a implementação tanto em modo transparente (camada 2) quanto em modo *gateway* (camada 3);

1.4.4. Possuir filtragem de pacote por endereço IP de origem e destino, por aplicação (independentemente da porta ou protocolo utilizados pela aplicação), também por sub-rede e por períodos do dia, permitindo a aplicação de regras por horários e por dias da semana;

1.4.5. Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;

1.4.6. Permitir a criação de zonas de segurança e criação de regras de *firewall* para a comunicação entre elas;

1.4.7. Ser otimizada para análise de conteúdo de aplicações em camada 7.

1.4.8. Permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.

1.4.9. Possuir mecanismo de *anti-spoofing*;

1.4.10. Permitir a criação de *VLANs* e suportar *VLAN trunking* no padrão IEEE 802.1q;

1.4.11. Deverá permitir a criação de pelo menos 50 interfaces lógicas associadas a *VLAN*;

1.4.12. Suportar agregação de links, conforme padrão IEEE 802.3ad;

1.4.13. Permitir o uso dos protocolos: NTP ou SNTP;

1.4.14. Suportar o redirecionamento de portas;

1.4.15. Suportar *Network Address Translation* (NAT 1-1, NAT 1-N, NAT N-1) de acordo com a RFC 3022, nos modos estático e dinâmico;

1.4.16. Possuir a funcionalidade de fazer tradução de endereços dinâmicos um-para-N, PAT (*Port Address Translation*);

1.4.17. Possuir funcionalidades de DHCP Cliente, Servidor e Relay;

1.4.18. Suportar os protocolos IPv4 e IPv6;

1.4.19. Suportar a inspeção *stateful* de tráfego IPv4 e IPv6;

1.4.20. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

1.4.21. Para IPv6, deve suportar roteamento estático e dinâmico;

1.4.22. Implementar a função de roteamento *multicast*;

1.4.23. Suportar o protocolo PIM (*Protocol Independent Multicast*);

1.4.24. Suportar aplicações multimídia como: H.323 e SIP;

1.4.25. Possuir interface gráfica (GUI);

1.4.26. Possuir interface de linha de comando acessível via SSH;

1.4.27. Possuir integração com Servidores de Autenticação RADIUS, LDAP e *Microsoft Active Directory* e local (base de usuários interna no equipamento) para criação de políticas, possibilitando a criação de regras de acesso/bloqueio utilizando:

1.4.27.1. Usuários;

1.4.27.2. Grupo de usuários;

1.4.27.3. Estações de trabalho;

1.4.27.4. Endereço IP;

1.4.27.5. Endereço de Rede;

1.4.27.6. Combinação das opções acima.

1.4.28. Implementar os padrões abertos de gerência de rede SNMPv1, SNMPv2 e SNMPv3;

1.4.29. Permitir o monitoramento SNMP, no mínimo, dos seguintes itens:

1.4.29.1. Desempenho total (*throughput*);

1.4.29.2. Conexões simultâneas;

1.4.29.3. Usuários autenticados;

1.4.29.4. Serviços habilitados ou desabilitados;

1.4.29.5. Quantidade de endereços distribuídos pelo DHCP;

1.4.30. Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura;

1.4.31. Deve permitir a delegação de funções de administração e registrar em log as ações dos usuários e administradores;

1.4.32. Permitir a realização de *backup* e *restore* das regras, configurações e políticas;

1.4.33. Deve registrar a identificação do usuário em todos os eventos associados gerados pelo equipamento, tais como: eventos de autenticação, registros de acesso ou bloqueio e eventos associados a ameaças.

1.5. Das funcionalidades de QoS, deve:

1.5.1. Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (*inbound/outbound*) através da classificação dos pacotes (*Traffic Shaping*);

1.5.2. Permitir a criação de políticas de QoS por:

1.5.2.1. Endereço de origem;

1.5.2.2. Endereço de destino;

1.5.2.3. Por usuário e grupo do LDAP/AD;

1.5.2.4. Por aplicações;

1.5.2.5. Por porta;

1.5.3. Com a finalidade de controlar todas as aplicações e tráfegos cujo consumo possa ser excessivo, como por exemplo aplicações de vídeo streaming como o Youtube, e o link ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicação, deve ter a capacidade de administrá-las por políticas de controle de largura de banda.

1.5.4. O QoS deve possibilitar a definição de limite de *Upload* e *Download* ou de classes por: banda garantida, banda máxima e fila de prioridade;

1.5.5. Permitir a priorização *Real Time* de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP.

1.6. Das funcionalidades de VPN, deve:

1.6.1. Suportar VPN *Site-to-Site* e *Client-To-Site*;

1.6.2. Suportar IPSec VPN;

1.6.3. Suportar SSL VPN *Client-to-site*;

1.6.4. Os equipamentos deverão ser fornecidos com o *software* cliente e as licenças para conexão de 25 usuários VPN SSL simultâneos.

1.6.5. A VPN IPSEc deve suportar: 3DES, Autenticação MD5 e SHA-1, *Diffie-Hellman Group 1*, *Group 2, Group 5* e *Group 14, Algoritmo Internet Key Exchange (IKE)*, AES 128 e 256 *(Advanced Encryption Standard)* e autenticação via certificado IKE PKI;

1.6.6. A VPN SSL deve suportar:

1.6.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB do tipo portal;

1.6.6.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

1.6.6.3. Atribuição de endereço IP nos clientes remotos de VPN;

1.6.6.4. Atribuição de DNS nos clientes remotos de VPN;

1.6.6.5. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

1.6.6.6. Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;

1.6.6.7. O agente de VPN SSL *client-to-site* deve ser compatível com pelo menos: Windows XP, Windows 7, Windows 8 e Windows 10.

1.7. Das funcionalidades de IPS, deve:

1.7.1. Possuir integração à plataforma de segurança e dispor de mecanismos para detectar e prevenir ataques baseados em anomalias de tráfego, protocolo e assinaturas;

1.7.2. Possuir tecnologia de detecção e prevenção de ataques e intrusões baseada em assinatura;

1.7.3. Ser capaz de operar como "IPS" (modo *in-line*).

1.7.4. Permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

1.7.5. Possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;

1.7.6. Proteção contra ataques de Windows;

1.7.7. Proteção contra ataques de SMTP (*Simple Message Transfer Protocol*), IMAP (*Internet Message Access Protocol, Sendmail* e POP (*Post Office Protocol*);

1.7.8. Proteção contra ataques DNS (*Domain Name System*);

1.7.9. Proteção contra ataques a FTP e SSH;

1.7.10. Proteção contra ataques de ICMP (*Internet Control Message Protocol)*;

1.7.11. Possuir capacidade de identificação e bloqueio de ataques do tipo de negação de serviço (DoS).

1.7.12. Possuir capacidade de detectar ataques do tipo "*SYN flood"* e "*UDP flood".*

1.7.13. Possuir capacidade para detectar e evitar técnicas de evasão, tais como "*HTTP header folding*", "*HTTP junk header*", "*Post request evasion*" entre outros.

1.7.14. Permitir a monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar *traps* de SNMP quando ocorrer um evento relevante para a correta operação da rede;

1.7.15. Prover notificação via alarmes na console de administração e e-mail;

1.7.16. A base de assinaturas deve ser atualizada automaticamente;

1.8. Das funcionalidades de Filtro de URL, deve:

1.8.1. Possuir base de dados de URLs, categorizadas pelo tipo de conteúdo;

1.8.2. Possuir pelo menos 50 categorias para classificação de sites de internet;

1.8.3. Possuir capacidade de restringir o acesso a URLs específicas e categorias;

1.8.4. Permitir a integração ao serviço de diretório padrão LDAP, reconhecendo contas e grupos de usuários cadastrados;

1.8.5. Permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP, endereço IP e sub-rede;

1.8.6. Permitir a criação de listas personalizadas de "URL's" permitidas (lista branca) e bloqueadas (lista negra).

1.8.7. Permitir, nas listas de URL criadas, a inserção de URLs por expressão regular, permitindo adicionar domínios, subdomínios ou sites;

1.8.8. Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;

1.8.9. Ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;

1.8.10. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.8.11. Permitir visualizar graficamente quais os sites acessados e as respectivas categorias, assim como a quantidade de sessões e tráfego relacionados a elas.

1.8.12. Ser possível a exibição de mensagens de bloqueio customizável pelos administradores da rede aos usuários em uma tentativa de acesso a recursos proibidos pela política de segurança configurada;

1.8.13. Permitir trabalhar com protocolo “HTTP” e “HTTPS”.

1.8.14. Permitir a monitoração do tráfego web mesmo sem a realização de bloqueio de acesso aos usuários;

1.8.15. As atualizações de base de assinaturas devem ser realizadas automaticamente e sem interromper a execução dos serviços.

1.9. Das funcionalidades de Controle de aplicações, deve:

1.9.1. Possuir solução de controle de aplicações integrado à solução de segurança;

1.9.2. Possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

1.9.3. Reconhecer no mínimo 1700 (Um mil e setecentas) aplicações diferentes;

1.9.4. Permitir o reconhecimento nativo e que seja feito o bloqueio de aplicações através de uma lista pré-definida do fabricante e

atualizável relacionados a pelo menos as seguintes categorias: Jogos; Mensageiros Instantâneos; *Peer-to-Peer* (P2P); Proxy; Áudio; Vídeo; VOIP; E-mail; Compartilhamento de arquivos; Redes Sociais; Acesso remoto; Protocolos de rede; *Update* de *softwares*;

1.9.5. Inspecionar o *payload* de pacote de dados com o objetivo de detectar através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

1.9.6. Ser possível efetuar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

1.9.7. Permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

1.9.8. Permitir identificar quais as aplicações que estão sendo utilizadas, assim como a quantidade de sessões e tráfego relacionadas a elas nos últimos minutos e horas.

1.9.9. Permitir a identificação de usuários e possuir a capacidade de integração com o serviço de diretório padrão LDAP reconhecendo grupos de usuários cadastrados;

1.9.10. Permitir a definição de política de permissões específicas para usuários (individual ou em grupos)

1.9.11. Ser possível limitar a banda (*download/upload*) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.

1.9.12. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante;

1.9.13. As atualizações de base de assinaturas devem ser realizadas automaticamente e sem interromper a execução dos serviços.

1.10. Das funcionalidades de prevenção contra malwares, deve:

1.10.1. Possuir funções de Antivírus, *Anti-malware* integrados no próprio equipamento;

1.10.2. Possuir antivírus em tempo real, para ambiente de *gateway* internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;

1.10.3. Suportar granularidade nas políticas de Antivírus e *Anti-malware*, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

1.10.4. Ser capaz de identificar e bloquear tráfego gerado por "*worms", "spyware" e "botnets*";

1.10.5. Permitir o bloqueio de malwares (*adware, spyware, hijackers, keyloggers, etc*.);

1.10.6. Detectar e bloquear a origem de *portscans*;

1.10.7. Permitir o bloqueio de *download* de arquivos por extensão e tipo de arquivo;

1.10.8. Permitir o bloqueio de *download* de arquivos por tamanho;

1.10.9. Permitir a inspeção em arquivos comprimidos que utilizam o algoritmo *deflate* (zip, gzip, etc.).

1.10.10. Suportar rastreamento de vírus em arquivos *.pdf;

1.10.11. As atualizações devem ser automáticas e realizadas sem interromper a execução dos serviços.

1.11. Das funcionalidades de Inspeção SSL/TLS, deve:

1.11.1. Possuir solução de Inspeção SSL/TLS integrado à solução de segurança;

1.11.2. Permitir a inspeção SSL possibilitando a decriptografia de tráfego de entrada e saída SSL e TLS;

1.11.3. Permitir a inspeção pelo menos dos protocolos: DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, SMTP, SSH, NetBIOS, SMB, POP3, POP3S, SIP e TFTP;

1.11.4. Possuir funcionalidade de exceção em inspeção SSL para sites do tipo pessoais e aplicações bancárias, não decriptando o tráfego dessas sessões.

1.12. Da garantia e suporte técnico:

1.12.1. A solução completa deve possuir garantia e suporte técnico por um período mínimo de 60 (sessenta) meses.

1.12.2. A contratada deve possuir serviço de forma centralizada para abertura de chamados em português, em caso de ocorrências de defeitos e/ou falhas relativos aos produtos fornecidos, podendo ser via *e-mail, website* ou telefone, no horário 8x5 (Segunda a sexta-feira das 08:00 às 18:00, exceto feriados).

1.12.3. Os appliances deverão ser fornecidos com garantia de 60 meses do fabricante, com reposição/entrega de equipamentos ou substituição avançada de peças no próximo dia útil (regime 8x5 *Next Business Day* (NBD));

1.12.4. Os serviços de suporte técnico deverão ser prestados pela contratada com possibilidade de a contratante também abrir chamados diretamente com o fabricante dos equipamentos durante todo o período vigente do contrato.

1.12.5. Para cada solicitação deverá haver um número único de protocolo, que será informado imediatamente ao contratante. Além de comprometer-se em manter os registros de todos os chamados constando as descrições dos problemas e enviar relatório com os chamados por período, sempre que solicitado pela contratante.

1.12.6. Durante o período de garantia a parte ou peça defeituosa deverão ser substituídas pela Contratada sem ônus para a Defensoria Pública do Estado do Paraná, salvo quando o defeito for provocado por uso inadequado dos equipamentos. A substituição da peça defeituosa, quando houver, deverá ser

realizada também pela Contratada. Caso seja necessário recolher o equipamento para testes em ambiente da contratada, o deslocamento do equipamento será às custas da Contratada.

1.12.7. Se houver necessidade de substituição, o Departamento de Informática da Defensoria Pública Estado do Paraná deverá ser consultado através do *e-mail* informatica@defensoria.pr.def.br para que indique o procedimento a ser realizado.

1.12.8. Os serviços de reparo dos equipamentos especificados deverão ser executados pela Contratada na sede Administrativa em Curitiba.

1.12.9. Deverá ser possível a obtenção de imagens e atualizações corretivas de software (*firmwares, patches e drivers*) dos equipamentos pelo fabricante da solução ofertada durante o período de vigência da garantia.

1.12.10. Deverão ser fornecidas todas as licenças descritas no item 1.1.3, e garantia de pelo menos 60 meses afim de manter todas as bases de assinaturas dos dois *appliances* sempre atualizadas e em pleno funcionamento durante todo o período de vigência do contrato.

2. Treinamento

2.1. Características gerais:

2.1.1. O treinamento oficial do fabricante da solução ofertada deverá ser ministrado pela Contratada em data a ser combinada com a Defensoria Pública do Estado do Paraná em até 30 dias após a assinatura do contrato.

2.1.2. O treinamento deverá ser ministrado por instrutor devidamente certificado pelo fabricante da solução ofertada, para 5 participantes que serão definidos pela Contratante.

2.1.3. O treinamento deverá ser realizado no Estado do Paraná, a ser definido pela Contratada.

2.1.4. Caso o treinamento ocorra fora do município de Curitiba, a Contratada deverá arcar integralmente com todos os custos de locomoção, hospedagem, passagens e alimentação de todos os participantes da DPPR sem qualquer ônus a Contratante.

2.1.5. O treinamento deverá conter a exposição de conteúdo teórico e práticas em "laboratório funcional"; "Laboratório funcional" refere-se a um ambiente com equipamentos de rede capaz de simular de forma prática aos participantes todos os temas que serão abordados no treinamento (Conteúdo programático listado no item 2.2).

2.1.6. A infraestrutura necessária para a efetiva realização do treinamento será de total responsabilidade da Contratada, não sendo admitida a cobrança de quaisquer ônus adicionais à DPPR.

2.1.7. Fazem parte da infraestrutura do treinamento: eventual locação de sala/equipamentos, montagem de ambiente de laboratório funcional, gastos com eventual deslocamento, alimentação e afins do ministrante, e demais gastos relacionados à completa realização do treinamento nos termos aqui descritos.

2.1.8. O treinamento deverá incluir os conhecimentos necessários para a configuração, operação e administração dos equipamentos, com enfoque teórico e prático. O material didático deve ser individual, e fornecido pela Contratada (impresso ou em PDF). O conteúdo ministrado deverá destacar casos práticos em ambientes de produção, e minimizar o conteúdo essencialmente teórico.

2.1.9. O treinamento deverá ser realizado em língua portuguesa, possuindo carga horária mínima de 30 (trinta) horas, com no máximo 6 (seis) horas diárias, e devendo abordar, pelo menos, os seguintes temas:

2.2. Conteúdo programático:

- Visão geral e configuração inicial do equipamento.
- Acessos via GUI, SSH;

- Conceitos e criação de zonas, objetos, NAT e regras do ambiente.
- Criação de regras de NAT estático e dinâmico;
- Criação de políticas de *firewall* e recursos gerais de segurança.
- Configuração de DMZ;
- Criação de *VLAN*'s e configuração de *VLAN*'s por Porta, Protocolo, IP Sub-rede;
- Roteamento estático e dinâmico;
- Configuração de QoS;
- Configuração de VPN IPSEC *site-to-site;*
- Configuração *de VPN client-to-site (*VPN SSL);
- Autenticação LDAP e integração com o *Microsoft Active Directory*;
- Configuração de cenários de Alta disponibilidade Ativo/Ativo e Ativo/Standby;
- Balanceamento de carga;
- Configuração de recursos de decriptografia e inspeção de tráfego criptografado;
- Conceitos e configuração de cada um dos seguintes recursos abaixo:
- Controle de aplicativos;
- Filtro de URL's;
- IPS;
- *Anti-malware*;
- Logging, monitoramento e alertas;
- Web Proxy;
- *Backup* e restauração;
- Relatórios;
- Diagnósticos e solução de problemas (*Troubleshooting*).

ePROTOCOLO

PROTOCOLO INTEGRADO DO ESTADO
Fls. 71a
Mov. 4

Documento: **EspecificacaotecnicaFirewall.pdf.**

Assinado digitalmente por: **Renan Kuster de Azevedo** em 27/11/2020 16:42.

Inserido ao protocolo **17.129.025-2** por: **Renan Kuster de Azevedo** em: 27/11/2020 16:41.

Documento assinado nos termos do art. 18 do Decreto Estadual 5389/2016.

A autenticidade deste documento pode ser validada no endereço: **https://www.eprotocolo.pr.gov.br/spiweb/validarAssinatura** com o código: **e9ab386e60190ae47bcef89e03d005da.**

Lista com alguns fornecedores da solução:

Redisul Informática Ltda.

licitacoes@redisul.com.br

crislaine.malavski@redisul.com.br

Seal Telecom

https://www.sealtelecom.com.br/site/

jrabitto@sealtelecom.com.br

Solo Network

https://www.solonetwork.com.br/home

rafael.lehmkuhl@solonetwork.com.br

Cylk Soluções em informática Ltda.

https://www.cylk.com.br/

Teltec

https://teltecsolutions.com.br/

UnderProtection

https://www.underprotection.com.br/contato/

ePROTOCOLO

PROTOCOLO INTEGRADO DO ESTADO
Fls. 72a
Mov. 5

Documento: **ListadefornecedoresFirewall.pdf**.

Assinado digitalmente por: **Renan Kuster de Azevedo** em 27/11/2020 16:42.

Inserido ao protocolo **17.129.025-2** por: **Renan Kuster de Azevedo** em: 27/11/2020 16:41.

Documento assinado nos termos do art. 18 do Decreto Estadual 5389/2016.

A autenticidade deste documento pode ser validada no endereço: **https://www.eprotocolo.pr.gov.br/spiweb/validarAssinatura** com o código: **1f4178bde20a1d1ddeb7b1360023f6ce**.

Procedimento n.º 17.129.025-2

DESPACHO

Trata-se de procedimento instaurado pelo Departamento de Informática, com fito na aquisição de uma estrutura corporativa de *Firewall* de próxima geração (NGFW) para a Defensoria Pública do Estado do Paraná (DPE-PR).

Considerando que se trata de importante solução para prover segurança ativa e proteção a todas as informações trafegadas pelos sistemas da DPE-PR, autorizo o prosseguimento do feito para a contratação do objeto, nos termos do artigo 21 da Resolução DPG n° 104/2020.

Fica o feito registrado com o nível de criticidade 2, segundo Resolução DPG 108/2020.

Realizem-se as anotações necessárias.

À CGA para instrução.

Curitiba, 30 de novembro de 2020.

NICHOLAS MOURA E SILVA
Coordenador de Planejamento

2) Declaração de existência de dotação orçamentária

INFORMAÇÃO Nº 082/2022/CDP Protocolo: 17.129.025-2

Propósito: Indicação de Recursos para a Execução da Despesa Orçamentária.

Referência	fl. 222	
OBJETO:	(LICITAÇÃO) Aquisição de 02 equipamentos (appliance - hardware dedicado) Next Generation Firewall (NGFW) incluindo softwares, licenças e treinamento para a solução com 05 participantes.	
VALOR TOTAL	R$ 119.060,17	
VALOR 2022:	R$ 21.961,45	*Treinamento decorrente da aquisição de equipamentos de TI.*
DOTAÇÃO:	0760.03.061.43.6009 / 95 / 3.3	Fundo da Defensoria Pública / Recursos de Outras Fontes / Outras Despesas Correntes
Fonte:	250	Diretamente Arrecadados
Detalhamento:	3.3.90.40.10	Serviços de Treinamento e Capacitação
VALOR	R$ 97.098,72	*Aquisição de equipamentos (incluídos softwares e licenças).*
DOTAÇÃO:	0760.03.061.43.6009 / 95 / 4.4	Fundo da Defensoria Pública / Recursos de Outras Fontes / Investimentos
Fonte:	250	Diretamente Arrecadados
Detalhamento:	4.4.90.52.35	Equipamentos de Processamento de Dados
Disponibilidade Orçamentária	Atesta-se a disponibilidade orçamentária do exercício 2022 com a emissão do pré-empenho da despesa, conforme documento anexo (SIAF).	
Disponibilidade Financeira	Considera-se haver a disponibilidade financeira com a execução da previsão da arrecadação de receitas próprias do Fundo da Defensoria Pública.	

Encaminha-se esta Indicação Orçamentária para apreciação do Coordenador de Planejamento.

Curitiba, data da assinatura digital.

Luciano Sousa
Gestão Orçamentária

ePROTOCOLO

PROTOCOLO INTEGRADO DO ESTADO
Fls. 282a
Mov. 70

Documento: **17.129.0252_IO_082.pdf**.

Assinatura Qualificada realizada por: **Luciano Bonamigo de Sousa** em 15/02/2022 12:54.

Inserido ao protocolo **17.129.025-2** por: **Luciano Bonamigo de Sousa** em: 15/02/2022 12:53.

Documento assinado nos termos do Art. 38 do Decreto Estadual nº 7304/2021.

A autenticidade deste documento pode ser validada no endereço: **https://www.eprotocolo.pr.gov.br/spiweb/validarAssinatura** com o código: **3fe4688029178fffc9f9127edc9ad24d**.

JD Edwards

LUCIANO BONAMIGO DE SOUSA
(JPD920)

SIAF > Despesa > Pré Empenho

Gerar Pré-Empenho - Acesso a Cabeçalhos de Pedidos

Personal Form: (No Personalization) Consulta: Todos os Registros

Linha (R) Ferramentas (T)

Registros 1 - 5

04

	Data de Criação	Credor	Pré-Empenho	Unidade Orçamentária	P/A/OE	Nat. Despesa/ Receita	Descr	*17.129.025-2* Detalhamento Histórico	No. da Licitação	Elemento de Despesa	Saldo Orçamento Anterior	Valor Total	Saldo Orçamento Posterior
◉	19/10/21	7	21000478	0760	6009	33904010	Serv. de Treinam. e Capac.	(LICITAÇÃO) Treinamento decorrente da aquisição de equipamentos (appliance - hardware dedicado) Next Generati...		40	2.035.314,58		2.013.353,13
○	19/10/21	7	21000480	0760	6009	44905235	Equip Processam Dados	(LICITAÇÃO) Aquisição de equipamentos (appliance - hardware dedicado) Next Generation Firewall (NGFW) incluin...		52	190.071,48		92.972,76
○	15/02/22	7	22000300	0760	6009	33903948	Serv Seleção e Treinam	(LICITAÇÃO) Treinamento presencial para utilização da ferramenta: aquisição de solução de proteção de rede base...		39	6.544.809,92		6.522.848,47
○	15/02/22	7	22000301	0760	6009	44905235	Equip Processam Dados	(LICITAÇÃO) Aquisição de equipamentos (appliance - hardware dedicado) Next Generation Firewall (NGFW) incluin...		52	781.041,20	97.098,72	683.942,48
○	15/02/22	7	22000302	0760	6009	33904010	Serv. de Treinam. e Capac.	(LICITAÇÃO) Treinamento presencial para utilização da ferramenta: aquisição de solução de proteção de rede base...		40	1.386.485,41	21.961,45	1.364.523,96

ePROTOCOLO

PROTOCOLO INTEGRADO DO ESTADO
Fls. 283a
Mov. 71

Documento: **17.129.0252_IO_082_anexo.pdf**.

Assinatura Qualificada realizada por: **Luciano Bonamigo de Sousa** em 15/02/2022 12:54.

Inserido ao protocolo **17.129.025-2** por: **Luciano Bonamigo de Sousa** em: 15/02/2022 12:53.

Documento assinado nos termos do Art. 38 do Decreto Estadual nº 7304/2021.

A autenticidade deste documento pode ser validada no endereço: **https://www.eprotocolo.pr.gov.br/spiweb/validarAssinatura** com o código: **4910e8efd7706055070ed0ca32a83367**.

Protocolo n.º 17.129.025-2

DESPACHO

1. Ciente da Informação Nº 082/2022/CDP atesto a consonância da despesa com o Planejamento Institucional.

2. Proceda-se à juntada da Declaração do Ordenador de Despesas.

3. Encaminhe-se ao DCA/Gestão de Editais.

Curitiba, data da assinatura digital.

NICHOLAS MOURA E SILVA
Coordenador de Planejamento

ePROTOCOLO

PROTOCOLO INTEGRADO DO ESTADO
Fls. 284a
Mov. 72

Documento: **17.129.0252_CDP_082_DCA.pdf.**

Assinatura Qualificada realizada por: **Nicholas Moura e Silva** em 15/02/2022 14:49.

Inserido ao protocolo **17.129.025-2** por: **Luciano Bonamigo de Sousa** em: 15/02/2022 12:54.

Documento assinado nos termos do Art. 38 do Decreto Estadual nº 7304/2021.

A autenticidade deste documento pode ser validada no endereço: **https://www.eprotocolo.pr.gov.br/spiweb/validarAssinatura** com o código: **a4b723379c151691b54baaa67f986ca8.**

DECLARAÇÃO DO ORDENADOR DE DESPESA

DECLARO que a despesa objeto deste Protocolo nº 17.129.025-2 possui adequação orçamentária e financeira com a Lei Orçamentária Anual de 2022, Lei nº 20.873/21, bem como compatibilidade com o Plano Plurianual 2020-2023, Lei nº 20.077/19, e com a Lei de Diretrizes Orçamentárias, Lei nº 20.648/21.

Curitiba, data da assinatura digital.

ANDRÉ RIBEIRO GIAMBERARDINO
Defensor Público-Geral do Estado do Paraná

ePROTOCOLO

PROTOCOLO INTEGRADO DO ESTADO
Fls. 285a
Mov. 73

Documento: **17.129.0252_DOD_082.pdf.**

Assinatura Qualificada realizada por: **Andre Ribeiro Giamberardino** em 15/02/2022 13:09.

Inserido ao protocolo **17.129.025-2** por: **Luciano Bonamigo de Sousa** em: 15/02/2022 12:54.

Documento assinado nos termos do Art. 38 do Decreto Estadual nº 7304/2021.

A autenticidade deste documento pode ser validada no endereço: **https://www.eprotocolo.pr.gov.br/spiweb/validarAssinatura** com o código: **6f96776db8702d886dc8b2e4c30b5ee1.**

3) Pesquisa de preço

QUADRO DE COTAÇÕES CONSOLIDADO

17.129.025-2 - Aquisição de estrutura de Firewall Corporativo									
QUANTIDADE	EMPRESA	Alerta Security		BLOCKBIT TECNOLOGIA LTDA		SIGMA TELECOM		MÉDIAS ARREDONDADAS	
	CNPJ	06.946.041/0001-51		02.423.535/0001-09					
	TELEFONE	(11) 3105-8655 / (11) 97603-7976		(11) 2165-8888		(41) 3360-6633 / (41) 99184-0303			
	RESPONSÁVEL	Eryanne Pereira		Leise ou Luciano		Eduardo Morais			
	E-MAIL	epereira@alertasecurity.com.br / contato@alertasecurity.com.br		lwinter@blockbit.com / lgodoy@blockbit.com / lrsilva@blockbit.com		eduardo.morais@sigmatelecom.com.br			
	ITENS	PREÇO UNIT.	PREÇO TOTAL	PREÇO UNIT.	PREÇO TOTAL	PREÇO UNIT.	PREÇO TOTAL	UNITÁRIAS	TOTAL
2	Appliance de NGFW e licenciamento, com garantia de 60 meses	R$ 60.249,86	R$ 120.499,72	R$ 47.000,00	R$ 94.000,00	R$ 38.398,21	R$ 76.796,42	R$ 48.549,36	R$ 97.098,72
5	Treinamento da solução ofertada aos servidores da DPE/PR	R$ 5.250,00	R$ 26.250,00	R$ 5.000,00	R$ 25.000,00	R$ 2.926,86	R$ 14.634,30	R$ 4.392,29	R$ 21.961,45
	PREÇO TOTAL	R$ 146.749,72		R$ 119.000,00		R$ 91.430,72		R$ 119.060,17	
		* 1 centavo de diferença para o orçamento				* 1 centavo de diferença para o orçamento			

Curitiba, 15/10/2021

4) Termo de referência

PROTOCOLO: 17.129.025-2

TERMO DE REFERÊNCIA PRELIMINAR

1. DO OBJETO

1.1. Aquisição de solução de Firewall corporativo para a Defensoria Pública do Estado do Paraná.

2. DO DETALHAMENTO DO OBJETO

2.1. Aquisição de Solução de Firewall baseada em appliance (hardware dedicado) com características de Next Generation Firewall (NGFW) incluindo todos os softwares e licenças de uso como: filtro de URL, controle de aplicações, VPN, IPS, proteção contra malwares e inspeção SSL, compondo em uma plataforma de segurança integrada e robusta de um único fabricante, em cenário de alta disponibilidade, com garantia de 60 meses tanto do hardware como das licenças.;

2.2. Não serão aceitos equipamentos de propósito genérico (PC's ou servidores ou máquinas virtuais) sobre os quais podem instalar e ou executar um sistema operacional regular como "*Microsoft Windows", "FreeBSD", "SUN Solaris", "Apple OS X"* ou "*GNU/Linux*".

ITEM	DESCRIÇÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL
01.	*Appliance* de NGFW e licenciamento conforme especificações deste documento, com garantia de 60 meses	02 unidades	R$	R$
03.	Treinamento da solução ofertada aos servidores da DPE/PR	05 pessoas	-	R$
*	**TOTAL**	-	R$	R$

2.3. A solução deve contemplar:

2.3.1. Solução de Firewall de próxima geração (NGFW) composta por, 2 equipamentos (Cenário de Alta Disponibilidade - Ativo/Standby (HA). A Licença de HA deverá estar inclusa e ser perpétua);

2.3.2. Garantia de 60 meses da Solução de Firewall de próxima geração (NGFW) e licenças;

2.3.3. IPS (Subscrição por pelo menos 60 meses);

2.3.4. Controle de aplicações (Subscrição por pelo menos 60 meses);

2.3.5. Filtro de URL (Subscrição por pelo menos 60 meses);

2.3.6. Proteção contra ameaças (Subscrição por pelo menos 60 meses.);

2.3.7. VPN IPSEC e SSL (Subscrição por pelo menos 60 meses);

2.3.8. Inspeção SSL. (Subscrição por pelo menos 60 meses).

2.4. Todas as funcionalidades citadas acima deverão ser providas em um único equipamento.

2.5. Os equipamentos (*appliances*) fornecidos para o cenário de Alta disponibilidade devem ser do mesmo fabricante, modelo e configuração.

2.6. Na data da proposta, nenhum dos modelos ofertados poderá estar listado no site do fabricante em como *end-of-life* ou *end-of-sale*.

2.7. Os equipamentos deverão ser fornecidos com todos os itens acessórios de *hardware*, *firmware* e *softwares* necessários à sua perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, *drivers*, programas de configuração, etc.

2.8. Os equipamentos deverão estar acompanhados de sua documentação técnica completa e atualizada, contendo os manuais, guias de instalação e outros pertinentes. A documentação deverá ser fornecida em sua forma original, não sendo aceitas cópias de qualquer tipo.

2.9. Todas as características exigidas deverão ser comprovadas, independente da descrição da proposta, por meio de documentos oficiais do fabricante, como catálogos, manuais e fichas de especificação técnica, sob pena, na falta destes, de não aceitação do equipamento ofertado.

2.10. Os modelos de equipamentos ofertados devem estar homologados pela ANATEL (Agência Nacional de Telecomunicações).

3. DAS ESPECIFICAÇÕES TÉCNICAS

3.1. Características de hardware:

3.1.1. O equipamento deve ser compatível com rack de largura padrão de 19 polegadas, padrão EIA-310, e ocupar no máximo 2U. Todos os acessórios necessários para a montagem no rack deverão acompanhar o produto, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

3.1.2. Possuir fonte de alimentação AC bivolt, com chaveamento automático ou manual (tensão na faixa de 100 a 240 Volts) e frequência (de 50/60Hz);

3.1.3. A Fonte deverá ser interna ao equipamento.

3.1.4. Possuir LEDs de identificação de atividades de status do sistema, de cada porta e de energia.

3.1.5. Possuir, no mínimo, 5 (cinco) interfaces de rede Gigabit Ethernet 10/100/1000 Base-TX.

3.1.6. Possuir, no mínimo, 1 (uma) interface de rede 10/100/1000 Gbps dedicada para gerenciamento.

3.1.7. Possuir pelo menos 1 (uma) porta console de conexão para acesso a interface de comando CLI especifica para esta finalidade, utilizando cabo do tipo serial RS-232 ou RJ-45;

3.1.8. Possuir pelo menos 1 (uma) porta do tipo USB 2.0 ou 3.0 (Universal Serial Bus).

3.1.9. Possuir um disco interno de no mínimo 32GB, do tipo SSD (*Solid-state drive*).

3.2. Dos Requisitos mínimos de capacidade e performance, deve:

3.2.1. Possuir "*Firewall*" com *throughput* mínimo de 3,3 Gbps para pacotes do tipo "UDP" de tamanho de 1.518 (Mil quinhentos e dezoito) bytes.

3.2.2. Possuir *throughput* mínimo de 700 Mbps de NFGW com as seguintes funcionalidades habilitadas simultaneamente, devidamente ativadas e atuantes: *Firewall*, Controle de aplicação, filtro de URL, IPS e *Anti-malware*.

3.2.3. Possuir *throughput* mínimo de 700 Mbps para tráfego IPS;

3.2.4. Possuir *throughput* mínimo de 500 Mbps para proteção contra vírus e malwares.

3.2.5. Possuir *throughput* mínimo de 500 Mbps para tráfego de VPN.

3.2.6. Suportar no mínimo 50 túneis de "VPN SSL" *"client to site*".

3.2.7. Os appliances devem vir licenciados com 25 licenças ou mais de cliente VPN SSL.

3.2.8. Suportar no mínimo 300.000 (trezentos mil) conexões simultâneas;

3.2.9. Suportar no mínimo 18.000 (dezoito mil) novas conexões por segundo;

3.2.10. Possuir a funcionalidade de balanceamento e contingência de links;

3.2.11. Deve ser capaz de operar em alta disponibilidade (HA) nos modos de redundância Ativo/Passivo ou Ativo/Ativo com divisão de cargas.

3.2.12. A licença de alta disponibilidade (HA) deve estar inclusa na solução e ser fornecida pelo FORNECEDOR.

3.2.13. Deve suportar cluster do tipo *Failover* (HA) com replicação da tabela de estado para que não haja perda de conexões em caso de falha;

3.2.14. O HA (modo de Alta-Disponibilidade) deve possibilitar a monitoração de falhas dos links.

3.2.15. A comprovação dos requisitos de capacidade e performance deve ser realizada com base em documentação oficial do fabricante da solução ofertada.

3.3. Das funcionalidades de firewall, deve:

3.3.1. Possuir tecnologia de *firewall* do tipo *Stateful*;

3.3.2. Deve permitir acesso à internet de forma segura e com registro de toda a atividade de entrada e saída de informações;

3.3.3. Deve suportar a implementação tanto em modo transparente (camada 2) quanto em modo *gateway* (camada 3);

3.3.4. Possuir filtragem de pacote por endereço IP de origem e destino, por aplicação (independentemente da porta ou protocolo utilizados pela aplicação), também por sub-rede e por períodos do dia, permitindo a aplicação de regras por horários e por dias da semana;

3.3.5. Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;

3.3.6. Permitir a criação de zonas de segurança e criação de regras de *firewall* para a comunicação entre elas;

3.3.7. Ser otimizada para análise de conteúdo de aplicações em camada 7.

3.3.8. Permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.

3.3.9. Possuir mecanismo de *anti-spoofing*;

3.3.10. Permitir a criação de *VLANs* e suportar *VLAN trunking* no padrão IEEE 802.1q;

3.3.11. Deverá permitir a criação de pelo menos 50 interfaces lógicas associadas a *VLAN*;

3.3.12. Suportar agregação de links, conforme padrão IEEE 802.3ad;

3.3.13. Permitir o uso dos protocolos: NTP ou SNTP;

3.3.14. Suportar o redirecionamento de portas;

3.3.15. Suportar *Network Address Translation* (NAT 1-1, NAT 1-N, NAT N-1) de acordo com a RFC 3022, nos modos estático e dinâmico;

3.3.16. Possuir a funcionalidade de fazer tradução de endereços dinâmicos um-para-N, PAT (*Port Address Translation*);

3.3.17. Possuir funcionalidades de DHCP Cliente, Servidor e Relay;

3.3.18. Suportar os protocolos IPv4 e IPv6;

3.3.19. Suportar a inspeção *stateful* de tráfego IPv4 e IPv6;

3.3.20. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

3.3.21. Para IPv6, deve suportar roteamento estático e dinâmico;

3.3.22. Implementar a função de roteamento *multicast*;

3.3.23. Suportar o protocolo PIM (*Protocol Independent Multicast*);

3.3.24. Suportar aplicações multimídia como: H.323 e SIP;

3.3.25. Possuir interface gráfica (GUI);

3.3.26. Possuir interface de linha de comando acessível via SSH;

3.3.27. Possuir integração com Servidores de Autenticação RADIUS, LDAP e *Microsoft Active Directory* e local (base de usuários interna no equipamento) para criação de políticas, possibilitando a criação de regras de acesso/bloqueio utilizando:

3.3.27.1. Usuários;

3.3.27.2. Grupo de usuários;

3.3.27.3. Estações de trabalho;

3.3.27.4. Endereço IP;

3.3.27.5. Endereço de Rede;

3.3.27.6. Combinação das opções acima.

3.3.28. Implementar os padrões abertos de gerência de rede SNMPv1, SNMPv2 e SNMPv3;

3.3.29. Permitir o monitoramento SNMP, no mínimo, dos seguintes itens:

3.3.29.1. Desempenho total (*throughput*);

3.3.29.2. Conexões simultâneas;

3.3.29.3. Usuários autenticados;

3.3.29.4. Serviços habilitados ou desabilitados;

3.3.29.5. Quantidade de endereços distribuídos pelo DHCP;

3.3.30. Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura;

3.3.31. Deve permitir a delegação de funções de administração e registrar em log as ações dos usuários e administradores;

3.3.32. Permitir a realização de *backup* e *restore* das regras, configurações e políticas;

3.3.33. Deve registrar a identificação do usuário em todos os eventos associados gerados pelo equipamento, tais como: eventos de autenticação, registros de acesso ou bloqueio e eventos associados a ameaças.

3.4. Das funcionalidades de QoS, deve:

3.4.1. Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (*inbound/outbound*) através da classificação dos pacotes (*Traffic Shaping*);

3.4.2. Permitir a criação de políticas de QoS por:

3.4.2.1. Endereço de origem;

3.4.2.2. Endereço de destino;

3.4.2.3. Por usuário e grupo do LDAP/AD;

3.4.2.4. Por aplicações;

3.4.2.5. Por porta;

3.4.3. Com a finalidade de controlar todas as aplicações e tráfegos cujo consumo possa ser excessivo, como por exemplo aplicações de vídeo streaming como o Youtube, e o link ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse

tipo de aplicação, deve ter a capacidade de administrá-las por políticas de controle de largura de banda.

3.4.4. O QoS deve possibilitar a definição de limite de *Upload* e *Download* ou de classes por: banda garantida, banda máxima e fila de prioridade;

3.4.5. Permitir a priorização *Real Time* de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP.

3.5. Das funcionalidades de VPN, deve:

3.5.1. Suportar VPN *Site-to-Site* e *Client-To-Site*;

3.5.2. Suportar IPSec VPN;

3.5.3. Suportar SSL VPN *Client-to-site*;

3.5.4. Os equipamentos deverão ser fornecidos com o *software* cliente e as licenças para conexão de 25 usuários VPN SSL simultâneos.

3.5.5. A VPN IPSEc deve suportar: 3DES, Autenticação MD5 e SHA-1, *Diffie-Hellman Group 1*, *Group 2, Group 5* e *Group 14, Algoritmo Internet Key Exchange (IKE)*, AES 128 e 256 *(Advanced Encryption Standard)* e autenticação via certificado IKE PKI;

3.5.6. A VPN SSL deve suportar:

3.5.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB do tipo portal;

3.5.6.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

3.5.6.3. Atribuição de endereço IP nos clientes remotos de VPN;

3.5.6.4. Atribuição de DNS nos clientes remotos de VPN;

3.5.6.5. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

3.5.6.6. Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;

3.5.6.7. O agente de VPN SSL *client-to-site* deve ser compatível com pelo menos: Windows XP, Windows 7, Windows 8 e Windows 10.

3.6. Das funcionalidades de IPS, deve:

3.6.1. Possuir integração à plataforma de segurança e dispor de mecanismos para detectar e prevenir ataques baseados em anomalias de tráfego, protocolo e assinaturas;

3.6.2. Possuir tecnologia de detecção e prevenção de ataques e intrusões baseada em assinatura;

3.6.3. Ser capaz de operar como "IPS" (modo *in-line*).

3.6.4. Permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

3.6.5. Possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;

3.6.6. Proteção contra ataques de Windows;

3.6.7. Proteção contra ataques de SMTP (*Simple Message Transfer Protocol*), IMAP (*Internet Message Access Protocol, Sendmail* e POP (*Post Office Protocol*);

3.6.8. Proteção contra ataques DNS (*Domain Name System*);

3.6.9. Proteção contra ataques a FTP e SSH;

3.6.10. Proteção contra ataques de ICMP (*Internet Control Message Protocol)*;

3.6.11. Possuir capacidade de identificação e bloqueio de ataques do tipo de negação de serviço (DoS).

3.6.12. Possuir capacidade de detectar ataques do tipo "*SYN flood"* e "*UDP flood".*

3.6.13. Possuir capacidade para detectar e evitar técnicas de evasão, tais como "*HTTP header folding*", "*HTTP junk header*", "*Post request evasion*" entre outros.

3.6.14. Permitir a monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar *traps* de SNMP quando ocorrer um evento relevante para a correta operação da rede;

3.6.15. Prover notificação via alarmes na console de administração e e-mail;

3.6.16. A base de assinaturas deve ser atualizada automaticamente;

3.7. <u>Das funcionalidades de Filtro de URL, deve:</u>

3.7.1. Possuir base de dados de URLs, categorizadas pelo tipo de conteúdo;

3.7.2. Possuir pelo menos 50 categorias para classificação de sites de internet;

3.7.3. Possuir capacidade de restringir o acesso a URLs específicas e categorias;

3.7.4. Permitir a integração ao serviço de diretório padrão LDAP, reconhecendo contas e grupos de usuários cadastrados;

3.7.5. Permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP, endereço IP e sub-rede;

3.7.6. Permitir a criação de listas personalizadas de "URL's" permitidas (lista branca) e bloqueadas (lista negra).

3.7.7. Permitir, nas listas de URL criadas, a inserção de URLs por expressão regular, permitindo adicionar domínios, subdomínios ou sites;

3.7.8. Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;

3.7.9. Ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;

3.7.10. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

3.7.11. Permitir visualizar graficamente quais os sites acessados e as respectivas categorias, assim como a quantidade de sessões e tráfego relacionados a elas.

3.7.12. Ser possível a exibição de mensagens de bloqueio customizável pelos administradores da rede aos usuários em uma tentativa de acesso a recursos proibidos pela política de segurança configurada;

3.7.13. Permitir trabalhar com protocolo "HTTP" e "HTTPS".

3.7.14. Permitir a monitoração do tráfego web mesmo sem a realização de bloqueio de acesso aos usuários;

3.7.15. As atualizações de base de assinaturas devem ser realizadas automaticamente e sem interromper a execução dos serviços.

3.8. <u>Das funcionalidades de Controle de aplicações, deve:</u>

3.8.1. Possuir solução de controle de aplicações integrado à solução de segurança;

3.8.2. Possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

3.8.3. Reconhecer no mínimo 1700 (Um mil e setecentas) aplicações diferentes;

3.8.4. Permitir o reconhecimento nativo e que seja feito o bloqueio de aplicações através de uma lista pré-definida do fabricante e atualizável relacionados a pelo menos as seguintes categorias: Jogos; Mensageiros Instantâneos; *Peer-to-Peer* (P2P); Proxy; Áudio; Vídeo; VOIP; E-mail; Compartilhamento de arquivos; Redes Sociais; Acesso remoto; Protocolos de rede; *Update* de *softwares*;

3.8.5. Inspecionar o *payload* de pacote de dados com o objetivo de detectar através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

3.8.6. Ser possível efetuar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

3.8.7. Permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

3.8.8. Permitir identificar quais as aplicações que estão sendo utilizadas, assim como a quantidade de sessões e tráfego relacionadas a elas nos últimos minutos e horas.

3.8.9. Permitir a identificação de usuários e possuir a capacidade de integração com o serviço de diretório padrão LDAP reconhecendo grupos de usuários cadastrados;

3.8.10. Permitir a definição de política de permissões específicas para usuários (individual ou em grupos)

3.8.11. Ser possível limitar a banda (*download/upload*) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.

3.8.12. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante;

3.8.13. As atualizações de base de assinaturas devem ser realizadas automaticamente e sem interromper a execução dos serviços.

3.9. Das funcionalidades de prevenção contra malwares, deve:

3.9.1. Possuir funções de Antivírus, *Anti-malware* integrados no próprio equipamento;

3.9.2. Possuir antivírus em tempo real, para ambiente de *gateway* internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;

3.9.3. Suportar granularidade nas políticas de Antivírus e *Anti-malware*, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

3.9.4. Ser capaz de identificar e bloquear tráfego gerado por "*worms", "spyware" e "botnets*";

3.9.5. Permitir o bloqueio de malwares (*adware, spyware, hijackers, keyloggers, etc*.);

3.9.6. Detectar e bloquear a origem de *portscans*;

3.9.7. Permitir o bloqueio de *download* de arquivos por extensão e tipo de arquivo;

3.9.8. Permitir o bloqueio de *download* de arquivos por tamanho;

3.9.9. Permitir a inspeção em arquivos comprimidos que utilizam o algoritmo *deflate* (zip, gzip, etc.).

3.9.10. Suportar rastreamento de vírus em arquivos *.pdf;

3.9.11. As atualizações devem ser automáticas e realizadas sem interromper a execução dos serviços.

3.10. Das funcionalidades de Inspeção SSL/TLS, deve:

3.10.1. Possuir solução de Inspeção SSL/TLS integrado à solução de segurança;

3.10.2. Permitir a inspeção SSL possibilitando a decriptografia de tráfego de entrada e saída SSL e TLS;

3.10.3. Permitir a inspeção pelo menos dos protocolos: DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, SMTP, SSH, NetBIOS, SMB, POP3, POP3S, SIP e TFTP;

3.10.4. Possuir funcionalidade de exceção em inspeção SSL para sites do tipo pessoais e aplicações bancárias, não decriptando o tráfego dessas sessões.

3.11. Da garantia:

3.11.1. A solução completa deve possuir garantia por um período de 60 (sessenta) meses.

3.11.2. O FORNECEDOR deve possuir serviço de forma centralizada para abertura de chamados em português, em caso de ocorrências de defeitos e/ou falhas relativos aos produtos fornecidos, podendo ser via

e-mail, website ou telefone, no horário 8x5 (Segunda a sexta-feira das 08:00 às 18:00, exceto feriados).

3.11.3. Os *appliances* deverão ser fornecidos com garantia de 60 meses do fabricante, com reposição/entrega de equipamentos ou substituição avançada de peças no próximo dia útil (regime 8x5 *Next Business Day* (NBD));

3.11.4. A garantia deverá prever a possibilidade de a DPE/PR também abrir chamados diretamente com o fabricante dos equipamentos durante todo o período de garantia.

3.11.5. Para cada solicitação deverá haver um número único de protocolo, que será informado imediatamente ao DPE/PR. Além de comprometer-se em manter os registros de todos os chamados constando as descrições dos problemas e enviar relatório com os chamados por período, sempre que solicitado pela DPE/PR.

3.11.6. Durante o período de garantia, a parte ou peça defeituosa deverão ser substituídas pelo FORNECEDOR sem ônus para a DPE/PR, salvo quando o defeito for provocado por uso inadequado dos equipamentos. A substituição do equipamento, quando houver, deverá ser realizada também pelo FORNECEDOR. Caso seja necessário recolher o equipamento para testes em ambiente do FORNECEDOR, o deslocamento do equipamento será às suas custas do FORNECEDOR.

3.11.7. Se houver necessidade de substituição/reposição de hardware, o Departamento de Informática da DPE/PR deverá ser consultado através do e-mail informatica@defensoria.pr.def.br para que indique o procedimento a ser realizado.

3.11.8. Os serviços de reparo dos equipamentos especificados deverão ser executados pelo FORNECEDOR na Sede Administrativa da Defensoria Pública do Paraná, localizada na Rua Mateus Leme, 1908, Centro Cívico, Curitiba/PR, CEP 80530-010.

3.11.9. Deverá ser possível a obtenção de imagens e atualizações corretivas de software (*firmwares, patches e drivers*) dos equipamentos pelo fabricante da solução ofertada durante o período de vigência da garantia.

3.11.10. Deverão ser fornecidas todas as licenças descritas no item 1.1.3, e garantia de 60 meses a fim de manter todas as bases de assinaturas dos dois *appliances* sempre atualizadas e em pleno funcionamento durante todo o período de vigência da garantia.

4. DO TREINAMENTO

4.1. O treinamento oficial do fabricante da solução ofertada deverá ser ministrado pelo FORNECEDOR em data a ser agendada com a Defensoria Pública do Estado do Paraná, e deve ser realizado em até 30 (trinta) dias após solicitação formal da DPE/PR. O agendamento deverá estar disponível para a DPE/PR em até 05 (cinco) dias a contar da entrega dos equipamentos pelo FORNECEDOR.

4.2. O treinamento deverá ser ministrado por instrutor devidamente certificado pelo fabricante da solução ofertada, para 05 (cinco) participantes, a serem indicados pela DPE/PR.

4.3. O treinamento deverá ser realizado no Estado do Paraná, em local a ser definido pelo FORNECEDOR.

4.4. Caso o treinamento ocorra fora do município de Curitiba, o FORNECEDOR deverá arcar integralmente com todos os custos de locomoção, hospedagem, passagens e alimentação de todos os participantes da DPE/PR, sem qualquer ônus adicional.

4.5. O treinamento deverá conter a exposição de conteúdo teórico e práticas em “laboratório funcional”;

4.5.1. “Laboratório funcional” refere-se a um ambiente com equipamentos de rede capaz de simular de forma prática aos participantes todos os temas que serão abordados no treinamento (conforme item 4.9).

4.6. A infraestrutura necessária para a efetiva realização do treinamento será de total responsabilidade do FORNECEDOR, não sendo admitida a cobrança de quaisquer ônus adicionais à DPE/PR.

4.7. Fazem parte da infraestrutura do treinamento: eventual locação de sala/equipamentos, montagem de ambiente de laboratório funcional, gastos com eventual deslocamento, alimentação e afins do ministrante, e demais gastos relacionados à completa realização do treinamento nos termos aqui descritos.

4.8. O treinamento deverá incluir os conhecimentos necessários para a configuração, operação e administração dos equipamentos, com enfoque teórico e prático. O material didático deve ser individual, e fornecido pela empresa (impresso ou em PDF). O conteúdo ministrado deverá destacar casos práticos em ambientes de produção, e minimizar o conteúdo essencialmente teórico.

4.9. O treinamento deverá ser realizado em língua portuguesa, possuindo carga horária mínima de 30 (trinta) horas, com no máximo 6 (seis) horas diárias, e devendo abordar, pelo menos, os seguintes temas:

4.9.1. Visão geral e configuração inicial do equipamento.

4.9.2. Acessos via GUI, SSH;

4.9.3. Conceitos e criação de zonas, objetos, NAT e regras do ambiente.

4.9.4. Criação de regras de NAT estático e dinâmico;

4.9.5. Criação de políticas de *firewall* e recursos gerais de segurança.

4.9.6. Configuração de DMZ;

4.9.7. Criação de *VLAN*'s e configuração de *VLAN*'s por Porta, Protocolo, IP Sub-rede;

4.9.8. Roteamento estático e dinâmico;

4.9.9. Configuração de QoS;

4.9.10. Configuração de VPN IPSEC *site-to-site;*

4.9.11. Configuração de VPN client-to-site (VPN SSL);

4.9.12. Autenticação LDAP e integração com o *Microsoft Active Directory*;

4.9.13. Configuração de cenários de Alta disponibilidade Ativo/Ativo e Ativo/Standby;

4.9.14. Balanceamento de carga;

4.9.15. Configuração de recursos de decriptografia e inspeção de tráfego criptografado;

4.9.16. Conceitos e configuração de cada um dos seguintes recursos abaixo:

4.9.16.1. Controle de aplicativos;

4.9.16.2. Filtro de URL's;

4.9.16.3. IPS;

4.9.16.4. *Anti-malware*;

4.9.16.5. Logging, monitoramento e alertas;

4.9.16.6. Web Proxy;

4.9.16.7. *Backup* e restauração;

4.9.16.8. Relatórios;

4.9.16.9. Diagnósticos e solução de problemas (*Troubleshooting*).

4.10. Após a conclusão do treinamento, o FORNECEDOR deverá prover certificado individual aos participantes dos cursos, em até 30 (trinta) dias após sua finalização. O certificado deverá estar redigido em língua portuguesa, contendo, no mínimo: instituição, nome do curso, carga horária, nome do treinando, e conteúdo abordado.

5. CONDIÇÕES GERAIS

5.1. Os produtos devem ser novos, de primeiro uso, sem a presença de vícios e entregues em embalagens lacradas, sem custo adicional para a DPE/PR.

5.2. O FORNECEDOR deverá disponibilizar pessoal capacitado, materiais, equipamentos e ferramentas necessárias à perfeita execução dos serviços.

5.3. O valor deverá abranger eventuais custos com transporte, não sendo admitida cobrança adicional de quaisquer serviços acessórios.

5.4. Não serão aceitos produtos em desacordo com as especificações técnicas contidas neste Termo de Referência, salvo se de melhor qualidade, e a critério da DPE/PR.

5.5. O FORNECEDOR responsabilizar-se-á por todo e qualquer encargo trabalhista de seus empregados, bem como pelo correto cumprimento de sua jornada e por acidentes ocorridos no exercício da atividade.

5.6. Os serviços que apresentarem vício de qualidade e/ou que estejam em desacordo com as especificações constantes neste Termo, poderão ser rejeitados, devendo ser corrigidos ou refeitos às custas do FORNECEDOR, sem prejuízo da aplicação de eventuais penalidades legais.

5.7. A emissão do documento de cobrança pelo FORNECEDOR não poderá ser conjugada, isto é, não poderá conter prestação de serviço e fornecimento de peças/materiais em um mesmo documento.

5.7.1. Caso o objeto da contratação inclua prestação de serviços e fornecimento de peças/materiais, dois documentos de cobrança deverão ser emitidos pela empresa: um referente à prestação de serviços e outro referente ao fornecimento de peças/materiais.

5.7.2. Documentos de cobrança referentes ao fornecimento de peças/materiais deverão ser claramente especificados, informando quantidade e valor unitário de cada peça/material.

5.7.3. Estas disposições se aplicam mesmo que a empresa seja optante pelo regime Simples e enquadrada no MEI.

6. DA ENTREGA

6.1. Todos os itens (appliances de firewall e licenças) deverão ser entregues em até 30 (trinta) dias, a contar do recebimento de ordem de fornecimento enviada pela DPE/PR.

6.1.1. Este prazo somente poderá ser dilatado, a critério exclusivo da DPE/PR, mediante solicitação formal da empresa, dentro do prazo de entrega e com motivação fundamentada pela empresa.

6.1.2. O requerimento de prorrogação do prazo de entrega não interrompe a contagem do prazo inicialmente estipulada.

6.2. A entrega deverá ocorrer na Sede Administrativa da Defensoria Pública do Paraná, localizada na Rua Mateus Leme, 1908, Centro Cívico, Curitiba/PR, CEP 80530-010, aos cuidados do Departamento de Informática.

6.3. A entrega deve ocorrer em dia útil (previamente acordado com o responsável pelo recebimento), em horário entre as 10h00 e as 16h00, ou conforme especificado.

6.4. Os itens entregues serão recebidos provisoriamente em até 15 (quinze) dias, e definitivamente em até 30 (trinta) dias.

6.5. Os serviços realizados serão recebidos provisoriamente em até 15 (quinze) dias e definitivamente em até 90 (noventa) dias.

6.6. O pagamento do serviço de treinamento será realizado em parcela única, após recebimento definitivo do objeto.

6.7. O pagamento dos equipamentos de hardware será realizado em parcela única, após recebimento definitivo do objeto.

6.8. O pagamento dos licenciamentos será realizado mensalmente.

7. DOS CRITÉRIOS DE SUSTENTABILIDADE

7.1. De acordo com o Art. 48 do Decreto Estadual no 4993, de 31 de agosto de 2016, as empresas adotarão as seguintes práticas de sustentabilidade, quando couber:

> I - Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme normas específicas da ABNT;
>
> II - Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO, como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;
>
> III - Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento; e

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

7.2. Também deverão ser observados, no que couber, os preceitos da Lei Estadual nº 20.132, de 20 de janeiro de 2020, que altera dispositivos da Lei no 15.608, de 16 de agosto de 2007, e da Lei Estadual n° 16.075/2009.

Curitiba, 29 de abril de 2021.

CAMILA F. R. WEINGRABER
Gestão de Contratações
Departamento de Compras e Aquisições

5) Parecer Jurídico

À Gestão de Editais - Departamento de Compras e Aquisições,

I. RELATÓRIO

1. Trata-se de procedimento instaurado pelo Departamento de Informática (DIF), com o fito de promover a aquisição de estrutura corporativa de firewall para a Defensoria Pública do Estado do Paraná (DPE/PR).

2. Por meio do despacho (fls. 02-03), o DIF promoveu a abertura do procedimento solicitando a aquisição de itens. Às fls. 04- 55 (Anexo I - fls. 56- 72) consta o estudo técnico preliminar, fundamentação e justificativas, bem como a ciência do Coordenador do Planejamento e autorização para prosseguimento da contratação (fl.73).

3. O Coordenador-Geral de Administração, definiu o rito de tramitação (fls.74-75). Anexado o Termo de Referência preliminar às fls. 81-96.

4. Foi inserida cópia da troca de e-mails com empresas e as suas cotações (fls. 148-220); quadro de cotações (mapa de preços - fl.221); Indicação de Recursos para a Execução da Despesa Orçamentária, fl.282.

5. A Coordenadoria de Planejamento autorizou o prosseguimento e atestou a consonância da despesa com o Planejamento Institucional (fl. 284). A Declaração do ordenador da despesa foi juntada na fl.285.

6. O DIF, às fls. 287- 292, saneou pontos importantes para elaboração do edital e a minuta do contrato.

7. Por fim, a manifestação do DCA (fls. 293-294) esclareceu algumas opções técnicas na realização da minuta de edital e seus anexos realizada (fls. 296-351),

bem como trouxe as resoluções que designam os pregoeiros (as) e as equipes de apoio (fls. 352-355).

8. Em atendimento à solicitação do CGA, vêm os presentes autos para avaliação acerca da instrução processual, minuta do contrato e do Edital de Licitação.

9. É o breve relatório.

II. FUNDAMENTAÇÃO

10. Trata-se de procedimento licitatório a ser realizado na modalidade pregão, na forma eletrônica, pelo tipo menor preço, apurado através do valor global do lote, conforme item 2.1 do Anexo IX da Minuta contratual (fl. 339 - verso).

11. O artigo 37, § 5º, da Lei Estadual nº 15.608/2007, disciplina que o pregão é a modalidade de licitação destinada à aquisição de bens e serviços comuns, assim considerados aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado (artigo 45 da Lei Estadual de Licitações).

12. A partir da conceituação legal do pregão, extrai-se que a adoção da referida modalidade licitatória se encontra compatível com a aquisição de estrutura corporativa de firewall para a Defensoria Pública do Estado do Paraná.

13. De igual modo, o tipo de licitação adotado (menor preço) também se encontra adequado, visto que decorre de expressa disposição legal. No caso, o artigo 49, inciso VII, da Lei Estadual nº 15.608/2007.

14. Outrossim, por se tratar de lote único, foi afastada a hipótese de criação de cota exclusiva para microempresas e empresas de pequeno porte (ME/EPP), com fundamento no art. 9º, § 1º, II, do Decreto Estadual nº 2.474/2015[1].

15. Entretanto, em caso de participação de microempresa (ME) ou empresa de pequeno porte (EPP), serão assegurados os benefícios da Lei Complementar nº 123/2006 para as pessoas jurídicas ou pessoas físicas que se identificarem como ME/EPP no campo apropriado do sistema nos termos da LC nº 123/2006 (item 6.5, 6.5.1 do edital - fl.298).

16. Veja-se que, por se tratar de licitação para aquisição de estrutura corporativa de *firewall* e treinamento de (5) cinco servidores da DPE/PR sobre o item adquirido, com dependência de futura verificação da garantia estendida pelo prazo de 60 (sessenta) meses, não é o caso de se utilizar do sistema de registro de preços, não se amoldando o presente certame aos incisos do artigo 23, § 3°, da Lei Estadual de Licitações nº 15.608/2007.

17. Ora, no presente caso, trata-se de aquisição estrutura corporativa de firewall e treinamento presencial, não havendo que se falar em decomposição em diversos lotes, nem tampouco em aquisição conforme as necessidades, na medida em que a Instituição não demandará nova contratação em futuro próximo, pois é bem de natureza durável.

18. Portanto, é inviável a utilização do sistema de registro de preços.

19. No que tange a participação de consórcios, a CGA, por meio do seu DCA, optou por vedar a participação de empresas em consórcio, e sua justificativa, adequada à realidade deste processo, foi apresentada à fl. 293- item 2.

20. Ademais, verifica-se da leitura do item 13 (Habilitação- fls.302-303), da minuta do edital, que não foi exigido atestado de capacidade técnico-operacional, por se tratar de "aquisição de produto padrão no mercado" (fl.294, item 5). Portanto, esta

[1]Art. 9.º Não se aplica o disposto nos arts. 6.º a 8.º deste Decreto quando: (...) § 1.º Para o disposto no inciso II deste artigo, considera-se não vantajosa a contratação quando: (...) II - causar grandes transtornos operacionais para o órgão ou entidade contratante, justificadamente.

Coordenadoria Jurídica, não vislumbra óbice a esse entendimento, **especificamente quanto à aquisição do produto**.

21. Neste sentido o TCE/PR decidiu recentemente ser possível a dispensa dos requisitos de capacidade técnico-operacional se o objeto da licitação apresentar baixa complexidade. Confira-se:

> EMENTA: Consulta. Qualificação técnica dos licitantes. Art. 30, caput, II, e §1º, I, da Lei nº 8.666/93. Capacidade técnico-operacional e capacidade técnico-profissional. Requisitos distintos. **1. Possibilidade de dispensa dos requisitos de capacidade técnico-operacional se o objeto da licitação apresentar baixa complexidade. Necessidade de motivação explícita e amparada em razões de ordem técnica.** 2. Desnecessidade de registro dos atestados relativos à qualificação técnico-operacional nas entidades profissionais competentes por falta de previsão legal ou regulamentar, aplicando-se o disposto no art. 30, §3º da Lei nº 8.666/93. 3. Exigência de registro na entidade profissional competente apenas de atestados de capacidade técnica profissional em licitações cujo objeto seja de obras e serviços de engenharia (amplo sentido). Impossibilidade de exigência de atestados técnicos em nome da empresa. Resposta positiva para os Quesitos 1 e 2 e negativa para o Quesito 3[2].

22. No entanto, há dubiedade no edital. Vejamos: "*14.6. Caso esteja sendo exigida a apresentação de atestado de capacidade técnica pelos licitantes, e havendo dúvida do Pregoeiro em relação à sua veracidade, serão solicitados documentos comprobatórios*" (fl.304).

23. Portanto, primeiramente é necessário fazer a distinção do atestado de capacidade técnico-operacional e capacidade técnico-profissional, conforme o entendimento do Tribunal de Contas da União. *In verbis:*

> A qualificação técnica abrange tanto a experiência empresarial quanto a experiência dos profissionais que irão executar o serviço. A primeira seria a capacidade técnico-operacional, abrangendo atributos próprios da empresa, desenvolvidos a partir do desempenho da atividade empresarial com a conjugação de diferentes fatores econômicos e de uma pluralidade de pessoas. A segunda é denominada capacidade técnico-profissional, referindo-se à existência de profissionais com acervo técnico compatível com a obra ou serviço de engenharia a ser licitado[3].

[2] Acordão - nº 828/19 - Tribunal Pleno. TCE/PR.
[3] Acórdão - nº 1332/2006-Tribunal Plenário. TCU.

24. Após esclarecida a diferença entre a qualificação técnica-operacional e profissional, é preciso verificar se, em se tratando de aquisição de treinamento presencial para solução ofertada a 5 servidores, é possível a dispensa do atestado de capacidade técnico-operacional.

25. O Tribunal de Contas da União já se manifestou sobre o assunto. *In verbis:*

> A administração deve ter as garantias necessárias de que a empresa possui as condições técnicas para a boa execução dos serviços. O objetivo, portanto, de se exigir em editais de licitações públicas atestados de qualificação técnica profissional e/ou operacional é comprovar que a empresa está apta a cumprir as obrigações assumidas com a Administração Pública e, dessa forma, garantir que o serviço seja executado com a devida qualidade. Para que se obtenha a proposta mais vantajosa é necessária a especificação do produto ou serviço adequada às reais necessidades da Administração e a formulação de exigências de qualificação técnica e econômico-financeira que não restrinjam a competição e propiciem a obtenção de preços compatíveis com os de mercado, mas que afastem empresas desqualificadas do certame[4].

26. No presente caso, trata-se de treinamento de aulas teóricas e práticas aos servidores públicos desta DPE/PR, e o valor estimado será de R$ 21.961,45 para o treinamento de 5 pessoas (fl. 311). O treinamento é um serviço que exige conhecimento técnico especializado e, por isso, é razoável exigir a demonstração de que a fornecedora do treinamento demonstre que "que possui as condições técnicas para a boa execução" do serviço agregado. Exigir o atestado técnico-profissional terá o fito de comprovar que a empresa detém conhecimento técnico, experiência e qualificações necessárias para a realização do treinamento.

27. Portanto, é necessário, pertinente e não ofende aos princípios licitatórios como a competitividade, isonomia e legalidade, e, recomenda-se que seja inserido em Edital o atestado de capacidade técnico-profissional, **como requisito para aplicação do treinamento**.

28. Em relação à qualificação econômico-financeira, verifica-se que o edital exigiu apenas a apresentação de certidão negativa de pendência de processos de falência, de recuperação judicial ou de execução patrimonial, dispensado o balanço

[4] Acórdão nº 1214/2013-Plenário. TCU.

patrimonial e demonstrações contábeis. Tal possibilidade tem, de fato, sido reconhecida pela jurisprudência. Nesse sentido:

> RECURSO ESPECIAL. ADMINISTRATIVO. LICITAÇÃO. EDITAL. ALEGATIVA DE VIOLAÇÃO AOS ARTIGOS 27, III E 31, I, DA LEI 8666/93. NÃO COMETIMENTO. REQUISITO DE COMPROVAÇÃO DE QUALIFICAÇÃO ECONÔMICO-FINANCEIRA CUMPRIDA DE ACORDO COM A EXIGÊNCIA DO EDITAL. RECURSO DESPROVIDO.
> 1. A comprovação de qualificação econômico-financeira das empresas licitantes pode ser aferida mediante a apresentação de outros documentos. **A Lei de Licitações não obriga a Administração a exigir, especificamente, para o cumprimento do referido requisito, que seja apresentado o balanço patrimonial e demonstrações contábeis, relativo ao último exercício social previsto na lei de licitações (art. 31, inc. I), para fins de habilitação**.
> 2. "In casu", a capacidade econômico-financeira foi comprovada por meio da apresentação da Certidão de Registro Cadastral e certidões de falência e concordata pela empresa vencedora do Certame em conformidade com o exigido pelo Edital.
> 3. Sem amparo jurídico a pretensão da recorrente de ser obrigatória a apresentação do balanço patrimonial e demonstrações contábeis do último exercício social, por expressa previsão legal. Na verdade, **não existe obrigação legal a exigir que os concorrentes esgotem todos os incisos do artigo 31, da Lei 8666/93**.
> 4. A impetrante, outrossim, não impugnou as exigências do edital e acatou, sem qualuqer protesto, a habilitação de todas as concorrentes.
> 5. Impossível, pelo efeito da preclusão, insurgir-se após o julgamento das propostas, contra as regras da licitação.
> 6. Recurso improvido[5].

29. No presente caso, como não houve tal exigência, entende-se que o afastamento do balanço cumpriu as exigências legais. Ademais, no caso, reputa-se adequada a justificativa apresentada no despacho de itens. 2- 4 (fls. 293- 294), no sentido de que os serviços não exigem investimentos volumosos para execução, bastando a apresentação das certidões mencionadas no art. 31, II, da Lei Geral de Licitações.

30. Em relação ao lote único, como se sabe, a leitura sistemática da Lei Geral de Licitações indica que o administrador público, sempre que possível, deve viabilizar o parcelamento da execução, entretanto, no presente caso, por se tratar do objeto de aquisição, firewall e treinamento, será adjudicado em lote único.

[5] (REsp 402.711/SP, Rel. Ministro JOSÉ DELGADO, PRIMEIRA TURMA, julgado em 11/06/2002, DJ 19/08/2002, p. 145).

31. Sobre o assunto, o ilustre Professor Jorge Ulisses Jacoby Fernandes, no Parecer nº 2086/00, elaborado no Processo nº 194/2000 do TCDF, ensina que:

> Desse modo a regra do parcelamento deve ser coordenada com o requisito que a própria lei definiu: só se pode falar em parcelamento quando há viabilidade técnica para sua adoção. Não se imagina, quando o objeto é fisicamente único, como um automóvel, que o administrador esteja vinculado a parcelar o objeto. Nesse sentido, um exame atento dos tipos de objeto licitados pela Administração Pública evidencia que embora sejam divisíveis, há interesse técnico na manutenção da unicidade, da licitação ou do item da mesma. Não é pois a simples divisibilidade, mas a viabilidade técnica que dirige o processo decisório. Observa-se que, na aplicação dessa norma, até pela disposição dos requisitos, fisicamente dispostos no seu conteúdo, a avaliação sob o aspecto técnico precede a avaliação sob o aspecto econômico. É a visão jurídica que se harmoniza com a lógica. Se um objeto, divisível, sob o aspecto econômico for mais vantajoso, mas houver inviabilidade técnica em que seja licitado em separado, de nada valerá a avaliação econômica. Imagine-se ainda esse elementar exemplo do automóvel: se por exemplo as peças isoladamente custassem mais barato, mesmo assim, seria recomendável o não parcelamento, pois sob o aspecto técnico é a visão do conjunto que iria definir a garantia do fabricante, o ajuste das partes compondo todo único, orgânico e harmônico. Por esse motivo, deve o bom administrador, primeiramente, avaliar se o objeto é divisível. Em caso afirmativo, o próximo passo será avaliar a conveniência técnica de que seja licitado inteiro ou dividido.

32. Ademais, o TCU se manifestou, no seguinte sentido:

> O TCU determinou ao Ministério da Fazenda que, nas licitações cujo objeto fosse divisível, previamente à definição da forma de adjudicação a ser adotada, realizasse estudos que comprovassem as vantagens técnicas e econômicas da compra em lote único, comparativamente à parcelada, a fim de atender ao disposto no art. 23, § 1º, da Lei nº 8.666/1993, e à Súmula/TCU nº 247[6].

33. Como se nota das regras acima, o parcelamento é obrigatório desde que "técnica e economicamente viável". Por viabilidade técnica entende-se a possibilidade de não divisão da execução do objeto sem prejuízo à integridade qualitativa.[7]

[6] Acórdão nº 3.140/2006-TCU1ª Câmara. item 9.2, TC-015.663/2006-9.

[7] **Marçal Justen Filho** exemplifica da seguinte maneira: "Não é possível desnaturar um certo objeto, fragmentando-o em contratações diversas e que importam o risco de impossibilidade de execução satisfatória. Se a Administração necessitar adquirir um veículo, não teria sentido licitar a compra por

34. Com relação a viabilidade econômica entende-se a ausência de risco de aumentar o preço unitário a ser pago pela Administração, tratando-se do não parcelamento como instrumento para aumento da competitividade e aproveitamento dos recursos disponíveis no mercado, em razão do sistema firewall e licenças e treinamento que não sejam possíveis a sua divisão[8].

35. No presente caso, verifica-se que o Administrador Público apresentou justificativa, conforme demonstrado em estudo técnico preliminar elaborado pelo Departamento de Informática, às manifestações contidas em fls.04-55. Assim, para realização da aquisição em lote único, está fundamentada e baseada na viabilidade técnica e econômica, juntada aos autos do procedimento do Edital do Pregão Eletrônico.

36. Diante do exposto, sanadas as ressalvas apontadas nos itens nº24-27, verifica-se que o procedimento observou as determinações contidas nos diversos incisos do artigo 3º da Lei Federal nº 10.520/02 e dos artigos 38, 40 e 55 da Lei Federal nº 8.666/93, bem como aquelas constantes dos diversos incisos dos artigos 49, 55, 69 e 99 da Lei Estadual nº 15.608/07, razão pela qual a fase interna, a minuta do edital e a minuta contratual se encontram consonantes com as disposições legais atinentes ao procedimento licitatório adotado.

37. Por oportuno, saliente-se a obrigatoriedade de observância do prazo mínimo de 8 (oito) dias úteis entre publicação do aviso e a data fixada no edital como limite para a apresentação das propostas, nos termos do que dispõem os artigos 54, inciso IV, da Lei Estadual nº 15.608/07 e 4º, inciso V, da Lei Federal nº 10.520/02.

partes (pneus, chassis, motor etc.)". **Comentários à Lei de Licitações e Contratos Administrativos. 16ª ed. São Paulo: RT, 2014, p. 366.**

[8] **Nas palavras de Jessé Torres: "(...)** o parcelamento da execução é desejável sempre que assim o recomendem dois fatores cumulativos: o 'melhor aproveitamento dos recursos disponíveis no mercado' e a 'ampliação da competitividade'. **Ocorrentes ambos, haverá conveniência para o interesse público em que se parcele a execução do objeto, que resultará em vantagem para a Administração".** Comentários à Lei de Licitações e Contratações da Administração Pública**. 8ª ed. Rio de Janeiro: Renovar, 2009, p. 277.**

III. CONCLUSÃO

38. Diante do exposto, sanadas as ressalvas apontadas nos itens nº 24- 27, não se vislumbram óbices ao prosseguimento do presente procedimento licitatório e à autorização de abertura de sua fase externa.

39. Por fim, remetem-se os autos ao DCA e, supridas as ressalvas, encaminhem-se os autos ao DPG.

40. É o parecer. À deliberação.

Curitiba, 15 de março de 2022.

RICARDO MILBRATH PADOIM:04306367924

Assinado de forma digital por RICARDO MILBRATH PADOIM:04306367924
Dados: 2022.03.15 17:31:58 -03'00'

RICARDO MILBRATH PADOIM
Coordenador Jurídico

6) Decisão administrativa de autorização do certame

Procedimento nº 17.129.025-2

DECISÃO

Trata-se de procedimento instaurado pelo Departamento de Informática (DIF) para a aquisição a aquisição de uma estrutura corporativa de Firewall de próxima geração (NGFW) para a Defensoria Pública do Estado do Paraná (DPEPR).

Segundo o Departamento de Informática, "*a demanda visa atender as necessidades atuais e futuras de sustentação da infraestrutura tecnológica e de segurança da informação da instituição, resultantes do crescimento de fluxo de dados e a necessidade de acesso externo a sistemas da intranet, como é o caso por exemplo do Solar que está sendo implementado pelo DIF, ferramenta para otimizar o processo de atendimento e tramitação de processos aos assistidos, o OTRS para gerenciar e automatizar todos processos de serviço e suporte ao cliente na área de Informática, dentre outros*".

O "Estudo Técnico Preliminar" foi juntado às fls. 04/55 e a "Especificação Técnica" às fls. 56/71.

A Coordenadoria de Planejamento estabeleceu o nível de criticidade 2 para o feito, segundo Resolução DPG 108/2020.

A Coordenadoria-Geral de Administração (CGA), em despacho às fls. 74/75, determinou o rito ordinário para a tramitação do procedimento e, posteriormente, houve a juntada aos autos do Termo de Referência Preliminar (fls. 81/96).

Após adequações, novo Termo de Referência Preliminar foi juntado às fls. 107/123 e a minuta contratual às fls. 124/136.

O Coordenador de Planejamento (CDP) opinou pelo prosseguimento do feito (fl. 139).

Os orçamentos encaminhados a esta Defensoria Pública constam às fls. 142/220, seguidos do quadro de cotações à fl. 221.

Às fls. 222/225, houve a juntada da indicação orçamentária, atestado de adequação da despesa com o Planejamento Institucional e Plano de Contingência e declaração do ordenador de despesas.

Após as devidas adequações, foi juntada versão final do Termo de Referência às fls. 231/254.

A minuta do edital e os respectivos anexos constam às fls. 296/351.

As Resoluções que designam a comissão permanente de licitação e os pregoeiros foram apresentadas às fls. 353/355.

Por fim, a Coordenadoria Jurídica, por meio do Parecer nº 47/2022/COJ/DPPR, informou não vislumbrar óbices ao prosseguimento do procedimento licitatório e à autorização da abertura da sua fase externa (fls. 356/365), salvo a necessidade de ajustar a minuta em seu item 13.1, "j", com o objetivo de inserir disposição relativa à qualificação técnico-profissional da empresa.

Nova minuta do edital foi juntada às fls. 367/423

Vieram os autos, é o relatório.

Conforme o parecer de fls. 356/423, a Coordenadoria Jurídica entendeu que a próxima fase do procedimento está apta a ser realizada, tendo em vista que estão presentes todos os requisitos legais para a continuidade do certame, salvo a necessidade de ajustar a minuta em seu item 13.1, "j", o que restou devidamente corrigido pelo Departamento de Compras e Aquisições (fls. 367/423).

Nesse sentido, o parecer jurídico abordou aspectos da legalidade de todo o procedimento.

Em relação à modalidade licitatória adotada (pregão), extrai-se que se encontra compatível com o objeto em questão, o que se demonstra pela facilidade de realizar as cotações do objeto.

De igual modo, o tipo de licitação adotado (menor preço) também se encontra adequado, visto que decorre de expressa disposição legal. No caso, os artigos 4º, inciso X, da Lei Federal nº 10.520/2002 e 49, inciso VII, da Lei Estadual nº 15.608/2007.

Verifica-se ainda que se trata de licitação para a contratação de objeto já previamente definido, sem dependência de futura verificação de necessidade, nem tampouco possibilidade de fracionamento em quantitativos.

Dessa forma, não é o caso de se utilizar do sistema de registro de preços, não se amoldando o presente certame ao art. 15, inciso II, da Lei de Licitações, tampouco aos incisos do seu artigo 23.

Diante do valor da contratação e por se tratar de lote único, não há como restringir o certame às empresas de pequeno porte e microempresas, nos termos do inciso I, do art. 48 da LC n° 123/20062.

No que tange à participação de consórcios, prevalece o entendimento segundo o qual o legislador, no art. 33, da Lei Federal n° 8.666/93, não estabeleceu qualquer obrigatoriedade. Exige-se apenas justificativa adequada para a exclusão, a qual foi devidamente apresentada (fl. 352).

Quanto à qualificação econômico-financeira exigida, foi prevista a obrigatoriedade da certidão negativa de pendência de processos de falência, de recuperação judicial ou de execução patrimonial, a fim de evitar maiores riscos ao adequado cumprimento do objeto por problemas financeiros da futura contratada.

A dispensa de balanço patrimonial e demonstrações contábeis se mostra acertada, pois a apresentação das certidões mencionadas no art. 31, II, da Lei Geral de Licitações se mostra suficiente.

A Coordenadoria Jurídica também destacou a necessidade de as licitantes comprovarem que possuem profissional devidamente certificado pelo fabricante da solução ofertada, apto a ministrar o treinamento previsto no Capítulo 4 do Termo de Referência.

Constam nos autos a Anotação Orçamentária e o atestado da sua consonância com o Planejamento Institucional e com o Plano de Contingenciamento.

Enfim, o documento jurídico atesta que a fase interna e a minuta do edital se encontram em consonância com as disposições legais atinentes ao procedimento licitatório adotado.

Desta forma, a considerar que se verifica a procedência dos fundamentos técnicos e jurídicos contidos nos autos e no Parecer Jurídico nº 47/2022/COJ/DPPR (fls. 356/365), acolho-o nesta oportunidade, dando conta de haver vantajosidade na contratação nos termos indicados no edital.

Ademais, resta claro nos autos o interesse e a conveniência através das justificativas apresentadas.

Assim, ante o exposto, havendo legalidade procedimental, interesse e conveniência, autorizo a continuidade do feito dando início à fase externa do procedimento.

Encaminhe-se os autos ao Departamento de Compras e Aquisições para dar prosseguimento ao feito.

Curitiba, data de inserção no sistema.