



TRIBUNAL REGIONAL ELEITORAL DO PARA
RUA JOÃO DIOGO, 288 - Bairro CAMPINA - CEP 66015902 - Belém - PA

TERMO DE REFERÊNCIA (TR)

1. OBJETO

1.1. OBJETO DA CONTRATAÇÃO

A presente licitação tem por objeto o registro de preços para eventual e futura a aquisição de solução de *Web Application Firewall* (WAF) e balanceamento de carga, incluindo prestação de serviços de instalação e configuração, treinamento especializado e serviço de operação assistida, com garantia técnica de 60 (sessenta) meses, de acordo com as especificações e quantitativos previstos neste Termo de Referência.

GRUPO 1 - SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF)				
ITEM	DESCRIÇÃO	CATMAT/ CATSER	UNIDADE DE MEDIDA	QUANT.
1	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE VIRTUAL, COM GARANTIA DE 60(SESENTA) MESES.	27464	UN	2
2	?FORNECIMENTO DE ?SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE FÍSICO, COM GARANTIA DE 60(SESENTA) MESES.	27472	UN	2
3	CAPACIDADE ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB	27464	UN	2
4	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	27324	UN	1
5	TREINAMENTO ESPECIALIZADO	27260	UN	6
6	SERVIÇO DE OPERAÇÃO ASSISTIDA	27324	UN	1

1.2. VALIDADE DA ATA: A Ata de Registro de Preços a ser gerada terá validade de 12 (doze) meses a partir da data de sua homologação.

1.3. Justificativa para o agrupamento de itens.

1.3.1. O agrupamento dos itens do objeto do presente Instrumento em lote, tem por objetivo a padronização da contratação uma vez que os itens agrupados possuem a mesma natureza técnica, o que resulta ainda na otimização de recursos humanos e financeiros no desenvolvimento das atividades relacionadas à gestão contratual, uma vez que o gerenciamento de número variado de fornecedores traz ineficiência e custo na gestão e fiscalização da contratação.

1.3.2. Além disso, em razão da complexidade da solução, a possibilidade do parcelamento torna o contrato técnica, econômica e administrativamente inviável ou provoca a perda de economia de escala. Neste sentido, justifica-se o agrupamento em lote, uma vez que entendemos ser a opção mais vantajosa à administração e satisfatória do ponto de vista da eficiência técnica, por manter a qualidade do projeto, haja vista que o gerenciamento e execução técnica permanece todo o tempo a cargo de um mesmo fornecedor.

1.3.3. Nesse diapasão, as vantagens seriam o maior nível de controle pela Administração na execução da prestação de serviços, a maior facilidade no cumprimento do cronograma preestabelecido, a observância dos prazos de entrega do objeto, concentração da responsabilidade pela execução a cargo de um

fornecedor e melhor garantia no acompanhamento dos resultados, para o objeto estabelecido neste Termo de Referência.

1.3.4. Isto posto, o agrupamento em lote visa garantir a compatibilidade técnica e operacional entre os componentes da solução, visto que haverá integração entre software e hardware existente no TRE-PA, serviços prestados, a contratação será realizada através de um único lote.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. DA JUSTIFICATIVA

Com o crescimento dos ataques cibernéticos e espionagem virtual aos quais as empresas privadas e os órgãos da administração pública, especialmente o judiciário, têm sido vítimas, torna-se urgente a necessidade de adoção de mecanismos de segurança da informação e a utilização de recursos de inspeção e proteção do tráfego de dados que auxiliem, de forma proativa, a prevenção e proteção dos sistemas, ante às vulnerabilidades encontradas em diversos vetores – redes (perímetro), sistemas e aplicativos, servidores de aplicação, e infraestrutura de orquestradores de containers.

Eventos recentes de ataques cibernéticos contra órgãos do Poder Judiciário demonstram o potencial desses atacantes e a necessidade cada vez maior de implementar ações preventivas, detectivas e corretivas, de forma organizada e colaborativa para minimizar os riscos e reduzir os impactos às organizações. No Brasil, a escalada de ataques cibernéticos motivou a cúpula do Poder Judiciário, por meio do CNJ, a criar o Comitê de Segurança Cibernética do Poder Judiciário - Portaria CNJ Nº 242/2020. Os normativos publicados pelo Conselho Nacional de Justiça impõem diretrizes e novas responsabilidades quanto à segurança da informação e proteção de dados, além de um conjunto de controles e atividades técnicas que tem o objetivo de estabelecer um novo paradigma de segurança cibernética para os Órgãos do Poder Judiciário.

Por estes motivos, uma das necessidades urgentes da Justiça Eleitoral é na adoção de mecanismos de segurança da informação e a utilização de recursos de inspeção e proteção do tráfego de dados que auxiliem, de forma proativa, a prevenção das vulnerabilidades encontradas em diversos vetores – redes (perímetro), sistemas de mensagens eletrônicas (e-mail), sistemas e aplicativos, servidores de aplicação, e infraestrutura de orquestradores de containers.

A atenção relativa à segurança deve ser dispensada não somente aos sistemas informatizados, mas também às informações que esses sistemas recebem, armazenam, processam, divulgam e descartam. Na atualidade, as informações, que são consideradas patrimônio para as organizações, estão sob constantes riscos, o que indica que os investimentos para a proteção desses ativos precisam ser compatíveis com a sua importância, a complexidade dos ataques e o nível de exposição ao risco. Com isso, a Segurança da Informação tornou-se um ponto crucial para a sobrevivência e credibilidade das instituições.

A Resolução TSE nº 23.644/2021, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, instituiu como princípio norteador a garantia da disponibilidade, integridade, confidencialidade, autenticidade, irretratabilidade e audibilidade das informações produzidas, recebidas, armazenadas, tratadas ou transmitidas pelos órgãos da Justiça Eleitoral, no exercício de suas atividades e funções. Deste modo, o conjunto de orientações que fundamentam a Resolução TSE nº 23.644/2021 estão em consonância com o objetivo dessa contratação

Neste cenário, a Justiça Eleitoral trata diariamente um grande volume de dados sensíveis, necessitando proteger e garantir a confidencialidade, disponibilidade e integridade destas informações. Assim, com a ampliação da disponibilização das soluções baseadas em serviços e protocolos que constituem a Web, principalmente, HTTP (HyperText Transfer Protocol) e HTTPS (HyperText Transfer Protocol Secure), tanto para acessos externos e internos, os aplicativos da Web passaram a suportar uma ampla gama de funções críticas em diversos sistemas que sustentam os negócios, incluindo sistemas de recursos humanos, transparência e consulta processual, sistemas que suportam processos administrativos e judiciais, dentre outros. Estes meios, uma vez vulneráveis, tornaram-se uma brecha para ataques, pois os hackers não só podem invadir e roubar os dados das organizações por meio de e-mails maliciosos, programas infectados ou links duvidosos, como também oferecer perigo por meio do tráfego online até o site ou aplicativo corporativo. Torna-se necessário a ampliação da segurança, uma vez que os sistemas online podem conter potenciais vetores que se tornam alvos para a exploração de falhas, resultando nos conhecidos ataques cibernéticos

Pelo exposto, é necessária a contratação de uma solução que possa, de forma customizada ao ambiente, interceptar e mitigar o risco inerente aos sistemas. O alvo dos atacantes geralmente são vulnerabilidades em sistemas desatualizados, legados ou com falhas no desenvolvimento. Por meio dessas brechas, são realizados diversos tipos de ataques, visando à espionagem, ao vazamento de dados, ao roubo ou sequestro de informações, ou ainda à quebra de integridade e disponibilidade do ambiente.

Além do risco de vazamento de dados sensíveis, existe a preocupação de que a sociedade perca a confiança nos serviços disponibilizados, entre outras inúmeras consequências à imagem do Tribunal. Para que seja alcançado o nível de segurança exigido nos dias atuais, é necessário investir em processos, sistemas e conhecimento específicos contra ameaças avançadas.

Diante disso, Estratégia Nacional de Cibersegurança TSE e TREs (2021 a 2024), no Eixo Estruturante E3: Ferramentas Automatizadas (Ferramentas de Segurança de Borda), apontou a necessidade de contratação e implantação de solução de segurança WAF que permita realizar a proteção das aplicações da Internet/Intranet. A solução WAF, ou Firewall de Aplicação Web, é uma solução que fica entre o site ou aplicativo e o restante da internet e a rede interna, funcionando como uma barreira que bloqueia e protege o ambiente de aplicações contra ataques de Hackers, Spammers, DDoS, Injeções SQL, proteção contra captura de dados sensíveis e roubo de credenciais, prevenção à atividade de robôs (bots) maliciosos e muito outros tipos de ataques cibernéticos conhecidos.

Adicionalmente, considerando a necessidade de redução da complexidade da operação e a consolidação dos serviços para as aplicações, bem como o crescente uso de soluções e arquiteturas de software baseadas em contêineres, torna-se necessário que a solução pretendida inclua solução de balanceamento de carga e que a mesma seja integrada ao ambiente de contêineres, visando equalizar a distribuição de carga de acessos aos sistemas, tanto em ambiente interno quanto externo, tanto no ambiente das aplicações modernas quanto das aplicações legadas, nos diversos servidores de aplicação disponíveis na infraestrutura da Justiça Eleitoral, garantindo os requisitos necessários de segurança, desempenho e disponibilidade, principalmente, para sistemas críticos.

2.2. MOTIVAÇÃO DA CONTRATAÇÃO E NECESSIDADES DE NEGÓCIO

2.2.1. Com base nas diretrizes definidas na Estratégia Nacional de Cibersegurança, definidas pelo Tribunal Superior Eleitoral (TSE), vários investimentos em Tecnologia da Informação e Comunicação (TIC) estão sendo realizados para modernizar sua infraestrutura de TIC, com a finalidade mitigar o risco de ataques cibernéticos.

2.2.2. Dessa forma, visando alinhamento estratégico e ganho em escalabilidade, disponibilidade, confiabilidade na entrega dos serviços prestados à sociedade, existe a necessidade de contratação de solução de Web Application Firewall (WAF), que, dentre outras funções, realize a proteção e o balanceamento tráfego de aplicações.

2.2.3. O balanceamento de aplicações, que permite o aumento da disponibilidade, fazendo com que os acessos sejam distribuídos entre os recursos de infraestrutura, de maneira a otimizar seu uso.

2.2.4. A função de proteção das aplicações (mecanismo de segurança), realiza a interceptação, inspeção e processamento das requisições entre o cliente e a aplicação. A partir de um conjunto de regras, o WAF classifica as requisições em maliciosas (que são geralmente bloqueadas) e não-maliciosas, isto é, que são encaminhadas até a aplicação, objetivando garantir uma camada de proteção adequada aos sistemas e dados armazenados no Data Center do Tribunal.

2.2.5. Propõe-se, para tanto, a aquisição de Solução de Segurança da Informação – Firewall de Aplicação Web (WAF), visando à segurança e ao bom desempenho das atividades no âmbito desta Justiça Especializada. Conforme exposto, a aquisição fundamenta-se em razão da necessidade de mitigar os inúmeros riscos inerentes aos sistemas informatizados disponibilizados no Portais Internet e Intranet do Tribunal e, conseqüentemente, aumentar a confiabilidade, integridade e a disponibilidade dos serviços oferecidos ao público interno e à sociedade, segundo as melhores práticas do mercado de segurança da informação.

2.2.6. A motivação da contratação se dá, portanto, com base nas seguintes necessidades:

- No quesito segurança, pelo oferecimento de uma camada adicional de defesa, protegendo os servidores que hospedam aplicações Web, e executando funções de segurança de proteção dos servidores internos

- contra ataques por usuários da internet;
- No quesito performance, pela melhoria de acesso às aplicações dos sistemas administrativos e judiciais, através do balanceamento de carga;
- Ampliar o controle de perímetro, por meio da inspeção e análise contínuo de tráfego das aplicações;
- Aprimorar os mecanismos de monitoramento e detecção de ataques;
- Proporcionar a prevenção e mitigação de Ameaças Cibernéticas;
- Contribuir para a redução da superfície de ataques cibernéticos da justiça eleitoral.

2.3. OBJETIVOS A SEREM ALCANÇADOS POR MEIO DA CONTRATAÇÃO

- 2.3.1. Garantir que o acesso lógico aos ativos seja gerenciado e protegido, por meio de mecanismos de segurança de perímetro;
- 2.3.2. Tornar a infraestrutura da Justiça Eleitoral mais segura e confiável;
- 2.3.3. Prover resiliência ao ambiente de produção;
- 2.3.4. Assegurar a redundância adequada ao porte do parque tecnológico do Regional.

2.4. OBJETIVO DA CONTRATAÇÃO

2.4.1. Trata-se de contratação de empresa para fornecimento de solução de Web Application Firewall (WAF), na modalidade de Appliance Virtual e Físico, acrescido de licenciamento adicional, serviços de configuração, instalação, transferência de conhecimento e Operação Assistida.

2.5. Alinhamento Estratégico

I - PEJEP 2021/2026 - Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados

- Índice de continuidade
 - Abrange a medição do percentual de disponibilidade e desempenho dos serviços de rede e sistemas informatizados.
- Índice de cumprimento de requisitos de Proteção de Dados
 - Mede o percentual de cumprimento da implantação dos requisitos relacionados à Proteção e Segurança de Dados.

II - Planejamento Estratégico de TI (PETI) 2019-2022.

- Perspectiva Recursos / Objetivo Estratégico 2 - Garantir a Modernização dos Serviços e Infraestrutura de TI
 - Indicadores Estratégicos:
 - 2.1 Índice de disponibilidade de serviços de rede e sistemas essenciais de TI TRE-PA
 - 2.2 Índice de indisponibilidade para acesso à rede da Justiça Eleitoral

III - Outros Referenciais Estratégicos

- Estratégia Nacional de Cibersegurança - 2021 a 2024 (TSE e TREs) - evento 1370070
 - Eixo Estruturante E3: Ferramentas Automatizadas
 - **item ID_F05 S / WAF - WEB APP. FIREWALL - INTRANET**
- Resolução Nº 396 de 07/06/2021, Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)
 - Portaria Nº 162 de 10/06/2021 - Protocolos e Manuais (ENSEC-PJ).

2.6. Referências aos Estudos Preliminares

- Evento 1483788 - Processo SEI 0008981-46.2021.6.14.8000

2.7. Referências Legais

- Portaria nº18456/2019, estabelece as diretrizes para a Gestão de Ativos de Tecnologia da Informação e Comunicações e institui o processo de gestão de configuração e ativos de TIC no âmbito do TRIBUNAL REGIONAL ELEITORAL DO PARÁ – TRE-PA;
- Resolução CNJ Nº 182/2013, dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ);
- Resolução CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
- Resolução TSE Nº 23.644, de 1º de julho de 2021, Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
- Lei 8.666/1993, regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.
- Instrução Normativa Nº 1, de 4 de abril de 2019. Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;
- Decreto 9.488/2018, altera o Decreto nº 7.892, de 23 de janeiro de 2013, que regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993, e o Decreto nº 7.579, de 11 de outubro de 2011, que dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal;

2.8. Classificação do Objeto

2.8.1. Objeto associado à contratação é considerado comum, pois apresenta padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

2.9. Relação entre a demanda prevista e a quantidade a ser contratada

2.9.1. A contratação tem por objetivo assegurar a proteção de aplicações WEB e informações sensíveis armazenadas nos servidores em produção deste Regional por meio solução de Web Appliaction Firewall. Para tanto, devido a necessidade da contratação, as quantidades abaixo foram estimadas durante a realização do Estudo Técnico Preliminar para compor o projeto em sua totalidade, com vistas a contratação da solução, serviços de implantação e treinamento, garantia técnica, bem como a necessidade de complementação de licenças da solução:

DEMANDA EXISTE	QTDE	DESCRIÇÃO DA SOLUÇÃO DE TI A SER CONTRATADA	JUSTIFICATIVAS
PROTEÇÃO DE APLICAÇÕES WEB PUBLICADAS NA INTERNET/INTRANET ,HOSPEDADAS NO DATA CENTER DO TRIBUNAL	2	CLUSTER/SOLUÇÃO DE PROCEÇÃO CAMADA 7 PARA APLICAÇÕES WEB, FIREWALL(WAF), DO TIPO APPLIANCE VIRTUAL.	Cluster de proteção (2 appliances) das aplicações WEB hospedadas no ambiente de produção (Data Center) do Tribunal, visando mitigar os riscos de ataque cibernético, com Garantia e suporte técnico do fabricante, período de 60(sessenta) meses, necessárias à manutenção da disponibilidade da solução. * O fornecedor deverá prover a solução na modalidade de appliance
	2	CLUSTER/SOLUÇÃO DE PROCEÇÃO CAMADA 7 PARA APLICAÇÕES WEB,	

		FIREWALL(WAF), DO TIPO APPLIANCE FÍSICO.	<i>Físico e Virtual, em razão da necessidade de cara Regional participe da Ata RP. ** Deverão ser fornecidas 2(duas) unidades da solução, em cada modalidade, para configuração do cluster; em razão da redundância do serviço.</i>
LICENCIAMENTO EXPANSÃO DE CAPACIDADE	2	CAPACIDADE ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB	Capacidade adicional para solução em Firewall de Aplicações WEB, visando a expansão de capacidade da Taxa de transferência (throughput) da solução.
SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	1	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	Implantação da solução, incluindo instalação e configuração no ambiente do Tribunal e repasse técnico-operacional básico da solução.
	6	TREINAMENTO ESPECIALIZADO	Capacitação da equipe técnica (até 6 servidores) para administração da solução, por meio de treinamento.
SUPERVISÃO DA SOLUÇÃO EM PRODUÇÃO APÓS A IMPLATAÇÃO	1	OPERAÇÃO ASSISTIDA	Serviço de operação assistida.

Tabela 2 - Levantamento da demanda e quantidades e solução/serviço de TI a ser contratado.

2.9.2. Além disso, foram mapeadas as seguintes premissas gerais para atendimento da demanda:

- A Solução deverá possuir gerenciamento e armazenamento dos dados na rede local do tribunal, com appliances próprios localizados e instalados na infraestrutura do cliente (on-premise);
- A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução;
- A CONTRATADA deverá ofertar a solução na modalidade de Appliance Físico e Appliance Virtual;
- A contratação deverá fornecer implantação da solução no ambiente do Tribunal e treinamento EAD;
- A CONTRATADA deverá ofertar Garantia do Fabricante por 60(sessenta) meses. A garantia refere-se ao período oficial de suporte da solução, fornecido por seu fabricante, compreendendo o fornecimento de atualizações e correções durante todo o ciclo de vida da versão fornecida do sistema operacional.

3 ESPECIFICAÇÃO TÉCNICA E QUANTIDADE

LOTE ÚNICO			
ITEM	DESCRIÇÃO	UNIDADE DE	QUANT.

		MEDIDA	
1	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE VIRTUAL, COM GARANTIA DE 60(SESENTA) MESES.	UN	2

3.1. A SOLUÇÃO DE WEB APPLICATION FIREWALL – WAF

3.1.1. Requisitos mínimos da solução:

3.1.2. A Solução de WEB APPLICATION FIREWALL- (WAF) deverá ser instalado no data center do CONTRATANTE, devendo observar os seguintes requisitos mínimos:

3.1.3. A solução deverá ser do tipo Appliance virtual, compatível com os virtualizadores hypervisor VMWARE ESXi 6.5+, KVM. e Hyper-V;

3.1.4. A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução.

3.1.5. A Solução deverá possuir gerenciamento e armazenamento dos dados na rede local do tribunal, com appliances próprios localizados e instalados na infraestrutura do cliente (on-premise)

3.1.6. Capacidade de inspecionar no mínimo 01 Gbps (Um gigabit por segundo) de tráfego web em camada 7;

3.1.7. Admitir no mínimo 30.000 (trinta mil) novas conexões por segundo em camada 7;

3.1.8. Admitir no mínimo 900 (novecentas) transações por segundo (TPS) SSL com chaves RSA 2048 bits;

3.1.9. Suportar 2.000.000 (dois milhões) de conexões concorrentes em camada 4;

3.1.10. Suportar e garantir a instalação em ambiente de alta disponibilidade:

3.1.11. Deve permitir a configuração da solução em alta disponibilidade, permitindo o funcionamento em cluster do tipo ativo-passivo e ativo-ativo.

3.1.12. A solução deve suportar mais do que dois elementos no cluster para sincronização de configuração de forma nativa a fim de permitir escalabilidade no futuro.

3.1.13. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime" e queda de sessões em caso de falha de uma das unidades.

3.1.14. Deve possuir redundância de dispositivos, de maneira que, em caso de falha de um dos equipamentos, o estado de todas as conexões seja remanejado para o equipamento redundante, preservando o estado original de todas as tabelas de conexões e de persistência.

3.1.15. O equipamento deve permitir a sincronização das configurações de forma automática.

3.1.16. Caso seja necessária uma interligação entre os equipamentos, a CONTRATADA será integralmente responsável por tal interligação, garantindo a performance necessária para o atendimento da solução.

3.1.17. O equipamento, quando habilitado para mais de uma função (Balanceamento, DNS, Web Application Firewall, etc), deverá permitir a definição da importância da função para cada tipo de funcionalidade;

3.1.18. Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, WAF, etc.

3.1.19. Fornecer recurso para o transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

3.1.20. Analisar e proteger tráfego HTTP/1.0, HTTP/1.1, HTTP/2.0 e HTTP/3;

3.1.21. Possuir suporte a IPv6;

3.1.22. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

3.1.23. Deve suportar, no mínimo, 1000 VLANs simultaneamente;

3.1.24. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

3.1.25. Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).

3.1.26. Assinar cookies digitalmente e editar endereços de URL ("URL Rewriting");

3.1.27. O equipamento deverá permitir a sincronização das configurações:

3.1.27.1.1. De forma automática;

3.1.27.1.2. Manualmente, forçando a sincronização apenas no momento desejado;

3.1.28. Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

3.1.28.1.1. Compartilhar a rede de heartbeat com a rede de dados;

3.1.28.1.2. Utilizar uma rede exclusiva para o heartbeat.

3.1.29. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;

3.1.30. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

3.1.31. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade

e flexibilidade no compartilhamento dos scripts.

3.1.32. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

3.1.33. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version

3.1.34. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.

3.1.35. Deve implementar configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para a interface de gerenciamento

3.1.36. Permitir acesso in-band via SSH

3.1.37. Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.

3.1.38. Possuir console de administração com interface gráfica remota segura atendendo os seguintes requisitos:

3.1.38.1.1. Permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e logs;

3.1.38.1.2. Permitir a replicação de configurações e a aplicação de atualização de softwares para os elementos dos nós do cluster;

3.1.39. Manter internamente múltiplos arquivos de configurações do sistema;

3.1.40. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;

3.1.41. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;

3.1.42. Deverá ser possível associar aos usuários de bases externas como RADIUS, LDAP e TACACS+ o nível de acesso;

3.1.43. Possuir Interface Gráfica via Web;

3.1.44. Possuir auto-complementação de comandos na CLI;

3.1.45. Possuir ajuda contextual;

3.1.46. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;

3.1.47. A Solução deve ter suporte a sFlow;

3.1.48. Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;

3.1.49. Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;

3.1.50. A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;

3.1.51. A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;

3.1.52. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);

3.1.53. Suportar a rollback de configuração e imagem;

3.1.54. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;

3.1.55. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;

3.1.56. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;

3.1.57. A interface Gráfica deverá permitir a reinicialização do equipamento;

3.1.58. Reinicialização do equipamento por comando na CLI;

3.1.59. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;

3.1.60. Possuir traps SNMP;

3.1.61. Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events;

3.1.62. Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;

3.1.63. Implementar Debugging: CLI via console e SSH;

3.1.64. Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

3.1.65. Permitir a criação de políticas diferenciadas por aplicação.

3.1.66. Deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;

3.1.67. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

3.1.68. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

- 3.1.69. Permitir as seguintes opções de implementação:
- 3.1.70. Monitoramento (sem bloqueio);
- 3.1.71. Proxy (reverso e transparente).
- 3.1.72. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;
- 3.1.73. Remover as mensagens de erro do conteúdo que será enviado aos usuários;
- 3.1.74. Em modo “monitoramento” (sem bloqueio), realizar análise e avaliação do tráfego, gerar relatórios com os dados analisados e simular bloqueios para efeito de avaliação;
- 3.1.75. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos;
- 3.1.76. Bloquear ataques aos servidores de aplicação, por meio dos seguintes recursos:
 - 3.1.76.1. Identificação, isolamento e bloqueio de ataques sofisticados sem impactar nas transações das aplicações;
 - 3.1.77. Possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;
 - 3.1.78. A solução deve suportar e fazer a proteção do tráfego de protocolo WebSocket.
 - 3.1.79. A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automática
 - 3.1.80. Permitir a utilização de modelo positivo de segurança para proteger contra ataques às aplicações HTTP e HTTPS, além de proteção contra- ataques conhecidos aos protocolos HTTP e HTTPS;
 - 3.1.81. Quando detectada uma tentativa de ataque bloquear de imediato o tráfego ou a sessão;
 - 3.1.82. Bloqueio com intermediação e interrupção da conexão;
 - 3.1.83. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;
 - 3.1.84. Utilização de página HTML informativa e personalizável como HTTP Response aos bloqueios;
 - 3.1.85. Configuração de políticas de bloqueio baseadas em requisição HTTP, endereço IP e usuário de aplicação;
 - 3.1.86. Permitir apenas transações de aplicações validadas, o restante das transações deverá ser bloqueado, utilizando bloqueio por nível de aplicação baseado no contexto da sessão do usuário, com privilégios de autorização diferentes, entradas de usuários e tempo de resposta de aplicação;
 - 3.1.87. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:
 - 3.1.87.1. Endereços IP que originaram os ataques;
 - 3.1.87.2. Horário do ataque;
 - 3.1.87.3. Nome do ataque;
 - 3.1.87.4. Qual campo foi atacado;
 - 3.1.87.5. Quantas vezes esse ataque foi realizado;
 - 3.1.88. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório), cookies, ações SOAP e elementos XML; identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP;
 - 3.1.89. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
 - 3.1.90. Identificar ataques baseados em:
 - 3.1.90.1. Assinaturas, com atualização diária da base pelo fabricante;
 - 3.1.90.2. Regras;
 - 3.1.90.3. Perfis de utilização;
 - 3.1.91. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado.
 - 3.1.92. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser auto-ajustáveis e adaptativos de acordo com mudanças.
 - 3.1.93. A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador.
 - 3.1.94. Detectar ataques de força bruta por meio dos seguintes métodos:
 - 3.1.95. Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;
 - 3.1.96. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP.
 - 3.1.97. Detectar ataques do tipo força bruta em que:
 - 3.1.97.1. O atacante solicita repetidamente o mesmo recurso;
 - 3.1.97.2. O atacante realiza repetidas tentativas não autorizadas de acesso;
 - 3.1.97.3. São utilizados ataques automatizados de login.
 - 3.1.98. Detectar ataques do tipo força bruta que explorem:
 - 3.1.98.1. Controles de acesso da aplicação (Erro 401 – Unauthorized);
 - 3.1.98.2. Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação;

- 3.1.98.3. Aplicações WEB que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação;
- 3.1.98.4. Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um range de Ips);
- 3.1.98.5. Clientes automatizados (robôs, requisições muito rápidas);
- 3.1.98.6. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
- 3.1.98.7. Possuir mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bidirecional atravessando o equipamento;
- 3.1.98.8. Possibilitar atualização de novas assinaturas para ataques conhecidos;
- 3.1.99. Apresentar proteção contra-ataques, como:
 - 3.1.99.1. Brute Force Login;
 - 3.1.99.2. Buffer Overflow;
 - 3.1.99.3. Cookie Injection;
 - 3.1.99.4. Cookie Poisoning;
 - 3.1.99.5. Cross Site Request Forgery (CSRF);
 - 3.1.99.6. Cross Site Scripting (XSS);
 - 3.1.99.7. Server Side Request Forgery (SSRF)
 - 3.1.99.8. Directory Traversal;
 - 3.1.99.9. Forceful Browsing;
 - 3.1.99.10. HTTP Denial of Service;
 - 3.1.99.11. HTTP hidden field manipulation;
 - 3.1.99.12. HTTP request smuggling;
 - 3.1.99.13. HTTP Response Splitting;
 - 3.1.99.14. Malicious Robots;
 - 3.1.99.15. Parameter Tampering;
 - 3.1.99.16. Remote File Inclusion Attacks;
 - 3.1.99.17. Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI);
 - 3.1.99.18. Session Hijacking;
 - 3.1.99.19. SQL Injection;
 - 3.1.99.20. Web Scraping;
 - 3.1.99.21. Web server software and operating system attacks;
 - 3.1.99.22. Web Services (XML) attacks;
- 3.1.100. Permitir configurar granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;
- 3.1.101. Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:
 - 3.1.101.1. Assinatura de ataque;
 - 3.1.101.2. Código de response;
 - 3.1.101.3. Conteúdo da cookie;
 - 3.1.101.4. Conteúdo do cabeçalho;
 - 3.1.101.5. Conteúdo do payload;
 - 3.1.101.6. Hostname;
 - 3.1.101.7. IP de origem;
 - 3.1.101.8. Método HTTP;
 - 3.1.101.9. Número de ocorrências em determinado intervalo de tempo;
 - 3.1.101.10. Parâmetro;
 - 3.1.101.11. User-agent (navegador);
- 3.1.102. Permitir a criação de assinaturas de ataques.
- 3.1.103. Reconhecer assinaturas seletivas, e filtros de ataque que devem proteger contra:
 - 3.1.103.1. Ataques de negação de serviços automatizados;
 - 3.1.103.2. Worms e vulnerabilidades conhecidas;
 - 3.1.103.3. Requests em objetos restritos;
- 3.1.104. Deve proteger contra ataques SSRF (Server Side RequestForgery);
- 3.1.105. A solução oferecida deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra.
- 3.1.106. Deve possuir um conjunto de assinaturas para cada tipo de tecnologia bem definidos e agrupados. Portanto permitindo selecionar as tecnologias da aplicação (Apache, PHP, Linux, SQL, etc) para automaticamente selecionar o conjunto de assinaturas que se aplica as mesmas;
- 3.1.107. Ao atualizar ou adicionar uma nova assinatura, a solução deve automaticamente colocar essa assinatura em modo "staging" para evitar falsos positivos e não bloquear tráfego válido. Depois de um período a mesma

deve automaticamente entrar em modo de bloqueio;

3.1.108. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (File Types);

3.1.109. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação, ou enviar para inspeção através do protocolo ICAP;

3.1.110. Deve possuir uma proteção proativa comportamental contra ataques automatizados por robôs e outras ferramentas de ataque;

3.1.111. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação;

3.1.112. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual;

3.1.113. Possuir método de mitigação de DoS L7 baseado em:

3.1.113.1. Descarte de todas as requisições de um determinado IP e/ou país suspeito;

3.1.113.2. CAPTCHA para suspeitos que ultrapassem os thresholds;

3.1.113.3. Defesa proativa contra Bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô;

3.1.114. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego, análise de dados e Machine Learning, com o stress do servidor de aplicação para determinar uma condição de DDoS;

3.1.115. Aprender o comportamento da aplicação:

3.1.115.1. Campos, valores, cookies e URLs;

3.1.116. Políticas sugeridas somente devem ser aplicadas após um período configurável;

3.1.117. Inspeccionar e monitorar até a camada de aplicação, todo tráfego de dados HTTP, incluindo cabeçalhos, campos de formulários e conteúdo, além de inspecionar os requests e responses;

3.1.118. Realizar as checagens em todos os tipos de entrada de dados, como URLs, formulários, cookies, campos ocultos e parâmetros, consultas (query), métodos HTTP, elementos XML e ações SOAP;

3.1.119. Proteger contra mensagens XML e SOAP malformadas;

3.1.120. Utilizar o campo HTTP X-Forwarded-For sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com NAT;

3.1.121. Remover as mensagens de erro do conteúdo que será enviado aos usuários;

3.1.122. Deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão;

3.1.123. Deverá permitir o cadastro de robôs que podem acessar a aplicação;

3.1.124. Deverá implementar proteção ao JSON (JavaScript Object Notation);

3.1.125. Implementar a segurança de web services, através dos seguintes métodos:

3.1.125.1. Criptografar/Decriptografar partes das mensagens SOAP;

3.1.125.2. Assinar digitalmente partes das mensagens SOAP;

3.1.125.3. Verificação de partes das mensagens SOAP;

3.1.126. Deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;

3.1.127. Deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;

3.1.128. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário. Deve proteger esses dados criptografados de malwares e keyloggers;

3.1.129. Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos. Esse nome de parâmetro deve ser mudado constantemente pela ferramenta para dificultar ataques direcionados;

3.1.130. Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal;

3.1.131. A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas do equipamento;

3.1.132. A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros como por exemplo: Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys, Quotium Seeker, HP Webinspect.

3.1.133. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:

3.1.133.1. Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade.

- 3.1.134. Deverá permitir o agendamento de relatórios a serem entregues por email;
- 3.1.135. Emitir os seguintes relatórios gráficos por:
 - 3.1.135.1. Política de segurança;
 - 3.1.135.2. Tipos de ataques;
 - 3.1.135.3. Violações;
 - 3.1.135.4. URL que foram atacadas;
 - 3.1.135.5. Endereços IP de origem;
 - 3.1.135.6. localização geográfica dos endereços IPs de origem;
 - 3.1.135.7. Severidade;
 - 3.1.135.8. Código de resposta;
 - 3.1.135.9. Métodos;
 - 3.1.135.10. Protocolos;
 - 3.1.135.11. Sessão;
- 3.1.136. Permitir a seleção de período para emissão dos relatórios,
- 3.1.137. Permitir a geração das seguintes informações, por período:
 - 3.1.137.1. Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;
 - 3.1.137.2. Informações estatísticas de quantidade de conexões completadas e bloqueadas;
 - 3.1.137.3. Informações estatísticas de fluxo de tráfego;
 - 3.1.137.4. Informações estatísticas de quantidade de sessões ou conexões;
- 3.1.138. Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: HTTP e HTTPS;
- 3.1.139. Deve possuir capacidade para definir que todo tráfego seja tunelado e permitir a utilização do protocolo padrão HTTPS com SSL como transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento
- 3.1.140. Deve possuir capacidade para definir servidor virtual em HTTPS com perfil cliente SSL/TLS padrão e redirecionar tráfego HTTP para HTTPS para um determinado servidor virtual;
- 3.1.141. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL/TLS sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor.
- 3.1.142. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado
- 3.1.143. A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:
 - 3.1.143.1. SSL session cache Timeout;
 - 3.1.143.2. Session Ticket;
 - 3.1.143.3. OCSP (Online Certificate Status Protocol) Stapling;
 - 3.1.143.4. Dynamic Record Sizing;
 - 3.1.143.5. ALPN (Application Layer Protocol Negotiation);
 - 3.1.143.6. Perfect Forward Secrecy;
- 3.1.144. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:
 - 3.1.144.1. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS;
 - 3.1.144.2. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS;
 - 3.1.144.3. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;
 - 3.1.144.4. Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS;
 - 3.1.144.5. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS.
- 3.1.145. Deve possibilitar a customização da interface gráfica da página de login e mensagens de apresentação ao usuário de acordo com o grupo a que pertença;
- 3.1.146. A solução deve oferecer ferramenta de Portal de Acesso de Usuários que permita que usuários acessem aplicações internas a partir de rede externas, implementando as funcionalidades de Single Sign-on e VPN-SSL, com os seguintes recursos:
 - 3.1.146.1. modo “Túnel por aplicação” onde o usuário estabelece túnel somente para o tráfego da aplicação, não sendo permitido outro tipo de tráfego dentro do mesmo túnel;
 - 3.1.146.2. modo “Portal” onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;
 - 3.1.146.3. modo “Network”, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP

- roteável pela rede interna;
- 3.1.146.4. Ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeram autenticação, fazendo cache das credenciais do usuário e utilizar a credencial correta para cada sistema;
- 3.1.147. Deverá ser capaz de autenticar usuários em bases de dados LDAP, Radius, Tacacs+, Kerberos e RSA SecurID;
- 3.1.148. Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware ou one-time passcode (OTP); Deve possuir capacidade para realizar proxy reverso com a finalidade de omitir a URI real, promovendo assim o acesso seguro as aplicações web internas;
- 3.1.149. Deverá prover acesso remoto através de VPN SSL para Microsoft Windows, Linux, dispositivos/ baseados em Android e iOS e MAC OSX;
- 3.1.150. Deve possuir capacidade para realizar verificações e validações no dispositivo do cliente antes de conceder acesso tais como versão do sistema operacional, antivírus instalado, certificados digitais instalados na máquina, firewall ativado;
- 3.1.151. Melhora da disponibilidade das aplicações através do balanceamento da entrada de tráfego deve possuir, ao menos, as seguintes características:
- 3.1.151.1.1. DNS autoritativo;
- 3.1.151.1.2. DNS secundário;
- 3.1.151.1.3. DNS resolver;
- 3.1.151.1.4. DNS cache;
- 3.1.151.1.5. Balanceamento de DNS servers;
- 3.1.151.1.6. DNSSEC;
- 3.1.152. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;
- 3.1.153. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;
- 3.1.154. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT
- 3.1.155. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;
- 3.1.156. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;
- 3.1.157. Deve prover as respostas a queries DNS da própria RAM CACHE
- 3.1.158. A solução deve ser capaz de realizar IP Anycast;
- 3.1.159. A solução deve ser capaz de realizar DNSSEC, independente da estrutura dos servidores DNS em uso
- 3.1.160. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;
- 3.1.161. Suportar pelo menos os seguintes algoritmos de balanceamento:
- 3.1.161.1. Round Robin;
- 3.1.161.2. Global Availability;
- 3.1.161.3. Ratio;
- 3.1.161.4. LDNS Persist;
- 3.1.161.5. Geografia;
- 3.1.161.6. Disponibilidade da Aplicação;
- 3.1.161.7. Capacidade do Virtual Server;
- 3.1.161.8. Least Connections;
- 3.1.161.9. Pacotes por segundo;
- 3.1.161.10. Round trip time;
- 3.1.161.11. Hops;
- 3.1.161.12. Packet Completion Rate;
- 3.1.161.13. QoS definido pelo usuário;
- 3.1.161.14. Kilobytes per Second;
- 3.1.162. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);
- 3.1.163. A solução deve suportar edns-client-subnet (ECS) para tanto responder requisições de clientes ou encaminhar requisições de clientes (screening).
- 3.1.164. Baseado no ECS DNS deve ser possível preservar o endereço IP da subnet do cliente ao invés do LDNS para tomar decisões .
- 3.1.165. A solução deve funcionar pelo menos das seguintes formas:
- 3.1.165.1. Usar o ECS para tomar decisões baseado em topologia (Subnets)
- 3.1.165.2. Injetar o ECS (proxy requests) para outros servidores DNS
- 3.1.166. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver (suporte ECS).

- 3.1.167. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;
- 3.1.168. Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);
- 3.1.169. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;
- 3.1.170. Permitir o balanceamento de aplicações em um pool de servidores, independentemente do hardware, sistema operacional e tipo de aplicação;
- 3.1.171. Suportar os seguintes métodos de balanceamento:
 - 3.1.171.1. Round Robin;
 - 3.1.171.2. Least Connection;
 - 3.1.171.3. Por peso.
 - 3.1.171.4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;
 - 3.1.171.5. Weighted Percentage dinâmico (baseado no número de conexões);
 - 3.1.171.6. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;
- 3.1.172. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web.
- 3.1.173. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
 - 3.1.173.1. Por cookie;
 - 3.1.173.2. Endereço de origem;
 - 3.1.173.3. Sessão SSL;
 - 3.1.173.4. Análise da URL acessada;
 - 3.1.173.5. Através de qualquer parâmetro do cabeçalho HTTP;
 - 3.1.173.6. Através da análise do MS Terminal Services Session (MSRDP)
 - 3.1.173.7. Através da análise do SIP Call ID ou Source IP;
 - 3.1.173.8. Através da análise de qualquer informação da porção de dados (camada 7);
- 3.1.174. O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:
 - 3.1.174.1. ICMP, TCP, HTTP, HTTPS;
 - 3.1.174.2. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;
- 3.1.175. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor;
- 3.1.176. Realizar Network Address Translation (NAT);
- 3.1.177. Realizar proteção contra syn flood;
- 3.1.178. Realizar as proteções de cabeçalho: X-Frame-Options, X-XSS-Protection, X-Content-Type-Options
- 3.1.179. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;
- 3.1.180. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.
 - 3.1.180.1. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.
 - 3.1.180.2. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.
- 3.1.181. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço
- 3.1.182. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;
- 3.1.183. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;
- 3.1.184. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;
- 3.1.185. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;
- 3.1.186. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico;
- 3.1.187. Realizar Network Address Translation (NAT);
- 3.1.188. Realizar Proteção contra Denial of Service (DoS);
- 3.1.189. Realizar Proteção contra Syn flood;
- 3.1.190. Realizar Limpeza de cabeçalho HTTP;
- 3.1.191. Deve possuir suporte a Link Layer Discovery Protocol (LLDP);
- 3.1.192. Deve ser possível enviar, pelo menos, as seguintes informações via LLDP:

- 3.1.193. Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size;
- 3.1.194. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;
- 3.1.195. Deve ser capaz de realizar DHCP relay;
- 3.1.196. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:
- 3.1.196.1. Tempo de resposta da aplicação;
- 3.1.196.2. Latência;
- 3.1.196.3. Conexões para conjunto de servidores, servidores individuais;
- 3.1.196.4. Por URL;
- 3.1.196.5. A solução deve ter suporte a TLS 1.3.

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANT
2	FORNECIMENTO DE ?SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE FÍSICO, COM GARANTIA DE 60(SESSENTA) MESES.	UN	2

3.2. Especificação técnica mínima

- 3.2.1. Os appliances físicos devem ser novos e de primeiro uso;
- 3.2.2. Os equipamentos devem ser fornecidos em modo appliance, com conjunto de hardware e software dedicados, não podendo ser servidor de uso genérico, e que atendam todas as funcionalidades descritas neste Termo de Referência.
- 3.2.3. Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não devem ser remanufaturados, recondicionados ou possuir reparos de qualquer espécie.
- 3.2.4. Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante.
- 3.2.5. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2Us do referido rack;
- 3.2.6. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos"), incluindo todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento do equipamento no rack;
- 3.2.7. Deve ser fornecido com todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento.
- 3.2.8. Dispor de fonte de alimentação redundante com tensão de entrada de 110V a 220V AC automática e frequência de 60Hz;
- 3.2.9. Possuir sistema operacional customizado especificamente para funções de Web Application Firewall, não podendo ser entregue appliance do tipo NGFW;
- 3.2.10. Possuir, no mínimo, 06 interfaces, sendo 02 de 10GE com conectores padrão SFP+ (SR) e 04 portas SFP e transceivers (SR ou UTP); Serão aceitas interfaces de maior capacidade, desde que possibilitem ser transformados em 10 GE (incluindo os cabos "breakout" de no mínimo 3 metros);
- 3.2.11. Possuir 01 interfaces 1GE, incluso interfaces de gerência com conectores padrão RJ45;
- 3.2.12. Todas as interfaces fornecidas devem estar licenciadas e habilitadas para uso imediato;
- 3.2.13. Possuir no mínimo de 8.000 Mbps de throughput em camada 7;
- 3.2.14. Possuir capacidade de 4.000 transações por segundo (TPS) em TLS padrão RSA (chaves de 2.048 bit);
- 3.2.15. Possuir no mínimo compressão em hardware de 5.000 Mbps em (tráfego HTTP/HTTPS);
- 3.2.16. Recursos de agregação de portas baseado no protocolo LACP, segundo o padrão IEEE 802.3ad;
- 3.2.17. Memória RAM mínima de 16 GB;
- 3.2.18. Disco rígido com capacidade de armazenamento interno e retenção de logs para análise ser de no mínimo 1TB;
- 3.2.19. Deve vir acompanhado de todas as licenças de software ou hardware necessárias para atendimento das funcionalidades exigidas neste caderno de especificações técnicas;
- 3.2.20. Todas as funcionalidades devem continuar ativas, mesmo após o término do termo de garantia e suporte técnico.
- 3.2.21. Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados seja realizada com aceleração em hardware, para não onerar o sistema
- 3.2.22. Suportar e garantir a instalação em ambiente de alta disponibilidade;
- 3.2.23. Deve permitir a configuração da solução em alta disponibilidade, permitindo o funcionamento em cluster do tipo ativo-passivo e ativo-ativo.

- 3.2.24. A solução deve suportar mais do que dois elementos no cluster para sincronização de configuração de forma nativa a fim de permitir escalabilidade no futuro.
- 3.2.25. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime" e queda de sessões em caso de falha de uma das unidades.
- 3.2.26. Deve possuir redundância de dispositivos, de maneira que, em caso de falha de um dos equipamentos, o estado de todas as conexões seja remanejado para o equipamento redundante, preservando o estado original de todas as tabelas de conexões e de persistência.
- 3.2.27. O equipamento deve permitir a sincronização das configurações de forma automática.
- 3.2.28. Caso seja necessária uma interligação entre os equipamentos, a CONTRATADA será integralmente responsável por tal interligação, garantindo a performance necessária para o atendimento da solução.
- 3.2.29. O equipamento, quando habilitado para mais de uma função (Balanceamento, DNS, Web Application Firewall, etc), deverá permitir a definição da importância da função para cada tipo de funcionalidade;
- 3.2.30. Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, WAF, etc.
- 3.2.31. Fornecer recurso para o transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;
- 3.2.32. Analisar e proteger tráfego HTTP/1.0, HTTP/1.1, HTTP/2.0 e HTTP/3;
- 3.2.33. Possuir suporte a IPv6;
- 3.2.34. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;
- 3.2.35. Deve suportar, no mínimo, 1000 VLANs simultaneamente;
- 3.2.36. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);
- 3.2.37. Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).
- 3.2.38. Assinar cookies digitalmente e editar endereços de URL ("URL Rewriting");
- 3.2.39. O equipamento deverá permitir a sincronização das configurações:
- 3.2.39.1.1. De forma automática;
- 3.2.39.1.2. Manualmente, forçando a sincronização apenas no momento desejado;
- 3.2.40. Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:
- 3.2.40.1.1. Compartilhar a rede de heartbeat com a rede de dados;
- 3.2.40.1.2. Utilizar uma rede exclusiva para o heartbeat.
- 3.2.41. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;
- 3.2.42. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.
- 3.2.43. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.
- 3.2.44. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:
- 3.2.45. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version
- 3.2.46. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.
- 3.2.47. Deve implementar configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para a interface de gerenciamento
- 3.2.48. Permitir acesso in-band via SSH
- 3.2.49. Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.
- 3.2.50. Possuir console de administração com interface gráfica remota segura atendendo os seguintes requisitos:
- 3.2.50.1.1. Permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e logs;
- 3.2.50.1.2. Permitir a replicação de configurações e a aplicação de atualização de softwares para os elementos dos nós do cluster;
- 3.2.51. Manter internamente múltiplos arquivos de configurações do sistema;
- 3.2.52. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;
- 3.2.53. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;

- 3.2.54. Deverá ser possível associar aos usuários de bases externas como RADIUS, LDAP e TACACS+ o nível de acesso;
- 3.2.55. Possuir Interface Gráfica via Web;
- 3.2.56. Possuir auto-complementação de comandos na CLI;
- 3.2.57. Possuir ajuda contextual;
- 3.2.58. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;
- 3.2.59. A Solução deve ter suporte a sFlow;
- 3.2.60. Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;
- 3.2.61. Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;
- 3.2.62. A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;
- 3.2.63. A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;
- 3.2.64. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);
- 3.2.65. Suportar a rollback de configuração e imagem;
- 3.2.66. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;
- 3.2.67. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;
- 3.2.68. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;
- 3.2.69. A interface Gráfica deverá permitir a reinicialização do equipamento;
- 3.2.70. Reinicialização do equipamento por comando na CLI;
- 3.2.71. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;
- 3.2.72. Possuir traps SNMP;
- 3.2.73. Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events;
- 3.2.74. Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;
- 3.2.75. Implementar Debugging: CLI via console e SSH;
- 3.2.76. Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
- 3.2.77. Permitir a criação de políticas diferenciadas por aplicação.
- 3.2.78. Deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;
- 3.2.79. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
- 3.2.80. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;
- 3.2.81. Permitir as seguintes opções de implementação:
- 3.2.82. Monitoramento (sem bloqueio);
- 3.2.83. Proxy (reverso e transparente).
- 3.2.84. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;
- 3.2.85. Remover as mensagens de erro do conteúdo que será enviado aos usuários;
- 3.2.86. Em modo “monitoramento” (sem bloqueio), realizar análise e avaliação do tráfego, gerar relatórios com os dados analisados e simular bloqueios para efeito de avaliação;
- 3.2.87. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos;
- 3.2.88. Bloquear ataques aos servidores de aplicação, por meio dos seguintes recursos:
- 3.2.88.1. Identificação, isolamento e bloqueio de ataques sofisticados sem impactar nas transações das aplicações;
- 3.2.89. Possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;
- 3.2.90. A solução deve suportar e fazer a proteção do tráfego de protocolo WebSocket.
- 3.2.91. A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automática
- 3.2.92. Permitir a utilização de modelo positivo de segurança para proteger contra ataques às aplicações HTTP e HTTPS, além de proteção contra- ataques conhecidos aos protocolos HTTP e HTTPS;
- 3.2.93. Quando detectada uma tentativa de ataque bloquear de imediato o tráfego ou a sessão;
- 3.2.94. Bloqueio com intermediação e interrupção da conexão;
- 3.2.95. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;
- 3.2.96. Utilização de página HTML informativa e personalizável como HTTP Response aos bloqueios;

- 3.2.97. Configuração de políticas de bloqueio baseadas em requisição HTTP, endereço IP e usuário de aplicação;
- 3.2.98. Permitir apenas transações de aplicações validadas, o restante das transações deverá ser bloqueado, utilizando bloqueio por nível de aplicação baseado no contexto da sessão do usuário, com privilégios de autorização diferentes, entradas de usuários e tempo de resposta de aplicação;
- 3.2.99. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:
 - 3.2.99.1. Endereços IP que originaram os ataques;
 - 3.2.99.2. Horário do ataque;
 - 3.2.99.3. Nome do ataque;
 - 3.2.99.4. Qual campo foi atacado;
 - 3.2.99.5. Quantas vezes esse ataque foi realizado;
- 3.2.100. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório), cookies, ações SOAP e elementos XML; identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP;
- 3.2.101. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
- 3.2.102. Identificar ataques baseados em:
 - 3.2.102.1. Assinaturas, com atualização diária da base pelo fabricante;
 - 3.2.102.2. Regras;
 - 3.2.102.3. Perfis de utilização;
- 3.2.103. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado.
- 3.2.104. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser auto-ajustáveis e adaptativos de acordo com mudanças.
- 3.2.105. A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador.
- 3.2.106. Detectar ataques de força bruta por meio dos seguintes métodos:
- 3.2.107. Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;
- 3.2.108. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP.
- 3.2.109. Detectar ataques do tipo força bruta em que:
 - 3.2.109.1. O atacante solicita repetidamente o mesmo recurso;
 - 3.2.109.2. O atacante realiza repetidas tentativas não autorizadas de acesso;
 - 3.2.109.3. São utilizados ataques automatizados de login.
- 3.2.110. Detectar ataques do tipo força bruta que explorem:
 - 3.2.110.1. Controles de acesso da aplicação (Erro 401 – Unauthorized);
 - 3.2.110.2. Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação;
 - 3.2.110.3. Aplicações WEB que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação;
 - 3.2.110.4. Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um range de Ips);
 - 3.2.110.5. Clientes automatizados (robôs, requisições muito rápidas);
 - 3.2.110.6. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
 - 3.2.110.7. Possuir mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bidirecional atravessando o equipamento;
 - 3.2.110.8. Possibilitar atualização de novas assinaturas para ataques conhecidos;
- 3.2.111. Apresentar proteção contra-ataques, como:
 - 3.2.111.1. Brute Force Login;
 - 3.2.111.2. Buffer Overflow;
 - 3.2.111.3. Cookie Injection;
 - 3.2.111.4. Cookie Poisoning;
 - 3.2.111.5. Cross Site Request Forgery (CSRF);
 - 3.2.111.6. Cross Site Scripting (XSS);
 - 3.2.111.7. Server Side Request Forgery (SSRF)
 - 3.2.111.8. Directory Traversal;
 - 3.2.111.9. Forceful Browsing;
 - 3.2.111.10. HTTP Denial of Service;
 - 3.2.111.11. HTTP hidden field manipulation;
 - 3.2.111.12. HTTP request smuggling;
 - 3.2.111.13. HTTP Response Splitting;
 - 3.2.111.14. Malicious Robots;

- 3.2.111.15. Parameter Tampering;
- 3.2.111.16. Remote File Inclusion Attacks;
- 3.2.111.17. Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI);
- 3.2.111.18. Session Hijacking;
- 3.2.111.19. SQL Injection;
- 3.2.111.20. Web Scraping;
- 3.2.111.21. Web server software and operating system attacks;
- 3.2.111.22. Web Services (XML) attacks;
- 3.2.112. Permitir configurar granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;
- 3.2.113. Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:
 - 3.2.113.1. Assinatura de ataque;
 - 3.2.113.2. Código de response;
 - 3.2.113.3. Conteúdo da cookie;
 - 3.2.113.4. Conteúdo do cabeçalho;
 - 3.2.113.5. Conteúdo do payload;
 - 3.2.113.6. Hostname;
 - 3.2.113.7. IP de origem;
 - 3.2.113.8. Método HTTP;
 - 3.2.113.9. Número de ocorrências em determinado intervalo de tempo;
 - 3.2.113.10. Parâmetro;
 - 3.2.113.11. User-agent (navegador);
- 3.2.114. Permitir a criação de assinaturas de ataques.
- 3.2.115. Reconhecer assinaturas seletivas, e filtros de ataque que devem proteger contra:
 - 3.2.115.1. Ataques de negação de serviços automatizados;
 - 3.2.115.2. Worms e vulnerabilidades conhecidas;
 - 3.2.115.3. Requests em objetos restritos;
- 3.2.116. Deve proteger contra ataques SSRF (Server Side RequestForgery);
- 3.2.117. A solução oferecida deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra.
- 3.2.118. Deve possuir um conjunto de assinaturas para cada tipo de tecnologia bem definidos e agrupados. Portanto permitindo selecionar as tecnologias da aplicação (Apache, PHP, Linux, SQL, etc) para automaticamente selecionar o conjunto de assinaturas que se aplica as mesmas;
- 3.2.119. Ao atualizar ou adicionar uma nova assinatura, a solução deve automaticamente colocar essa assinatura em modo “staging” para evitar falsos positivos e não bloquear tráfego válido. Depois de um período a mesma deve automaticamente entrar em modo de bloqueio;
- 3.2.120. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (File Types);
- 3.2.121. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação, ou enviar para inspeção através do protocolo ICAP;
- 3.2.122. Deve possuir uma proteção proativa comportamental contra ataques automatizados por robôs e outras ferramentas de ataque;
- 3.2.123. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação;
- 3.2.124. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual;
- 3.2.125. Possuir método de mitigação de DoS L7 baseado em:
 - 3.2.125.1. Descarte de todas as requisições de um determinado IP e/ou país suspeito;
 - 3.2.125.2. CAPTCHA para suspeitos que ultrapassem os thresholds;
 - 3.2.125.3. Defesa proativa contra Bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô;
- 3.2.126. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego, análise de dados e Machine Learning, com o stress do servidor de aplicação para determinar uma condição de DDoS;
- 3.2.127. Aprender o comportamento da aplicação:
 - 3.2.127.1. Campos, valores, cookies e URLs;
- 3.2.128. Políticas sugeridas somente devem ser aplicadas após um período configurável;
- 3.2.129. Inspeccionar e monitorar até a camada de aplicação, todo tráfego de dados HTTP, incluindo cabeçalhos, campos de formulários e conteúdo, além de inspecionar os requests e responses;

- 3.2.130. Realizar as checagens em todos os tipos de entrada de dados, como URLs, formulários, cookies, campos ocultos e parâmetros, consultas (query), métodos HTTP, elementos XML e ações SOAP;
- 3.2.131. Proteger contra mensagens XML e SOAP malformadas;
- 3.2.132. Utilizar o campo HTTP X-Forwarded-For sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com NAT;
- 3.2.133. Remover as mensagens de erro do conteúdo que será enviado aos usuários;
- 3.2.134. Deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão;
- 3.2.135. Deverá permitir o cadastro de robôs que podem acessar a aplicação;
- 3.2.136. Deverá implementar proteção ao JSON (JavaScript Object Notation);
- 3.2.137. Implementar a segurança de web services, através dos seguintes métodos:
 - 3.2.137.1. Criptografar/Decriptografar partes das mensagens SOAP;
 - 3.2.137.2. Assinar digitalmente partes das mensagens SOAP;
 - 3.2.137.3. Verificação de partes das mensagens SOAP;
- 3.2.138. Deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;
- 3.2.139. Deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;
- 3.2.140. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário. Deve proteger esses dados criptografados de malwares e keyloggers;
- 3.2.141. Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos. Esse nome de parâmetro deve ser mudado constantemente pela ferramenta para dificultar ataques direcionados;
- 3.2.142. Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal;
- 3.2.143. A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas do equipamento;
- 3.2.144. A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros como por exemplo: Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys, Quotium Seeker, HP Webinspect.
- 3.2.145. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:
 - 3.2.145.1. Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade.
- 3.2.146. Deverá permitir o agendamento de relatórios a serem entregues por email;
- 3.2.147. Emitir os seguintes relatórios gráficos dos alterar por:
 - 3.2.147.1. Política de segurança;
 - 3.2.147.2. Tipos de ataques;
 - 3.2.147.3. Violações;
 - 3.2.147.4. URL que foram atacadas;
 - 3.2.147.5. Endereços IP de origem;
 - 3.2.147.6. localização geográfica dos endereços IPs de origem;
 - 3.2.147.7. Severidade;
 - 3.2.147.8. Código de resposta;
 - 3.2.147.9. Métodos;
 - 3.2.147.10. Protocolos;
 - 3.2.147.11. Sessão;
- 3.2.148. Permitir a seleção de período para emissão dos relatórios;
- 3.2.149. Permitir a geração das seguintes informações, por período:
 - 3.2.149.1. Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;
 - 3.2.149.2. Informações estatísticas de quantidade de conexões completadas e bloqueadas;
 - 3.2.149.3. Informações estatísticas de fluxo de tráfego;
 - 3.2.149.4. Informações estatísticas de quantidade de sessões ou conexões;
- 3.2.150. Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: HTTP e HTTPS;
- 3.2.151. Deve possuir capacidade para definir que todo tráfego seja tunelado e permitir a utilização do protocolo padrão HTTPS com SSL como transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento

- 3.2.152. Deve possuir capacidade para definir servidor virtual em HTTPS com perfil cliente SSL/TLS padrão e redirecionar tráfego HTTP para HTTPS para um determinado servidor virtual;
- 3.2.153. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL/TLS sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor.
- 3.2.154. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado
- 3.2.155. A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:
- 3.2.155.1. SSL session cache Timeout;
- 3.2.155.2. Session Ticket;
- 3.2.155.3. OCSP (Online Certificate Status Protocol) Stapling;
- 3.2.155.4. Dynamic Record Sizing;
- 3.2.155.5. ALPN (Application Layer Protocol Negotiation);
- 3.2.155.6. Perfect Forward Secrecy;
- 3.2.156. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:
- 3.2.156.1. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS;
- 3.2.156.2. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS;
- 3.2.156.3. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;
- 3.2.156.4. Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS;
- 3.2.156.5. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS.
- 3.2.157. Deve possibilitar a customização da interface gráfica da página de login e mensagens de apresentação ao usuário de acordo com o grupo que pertença;
- 3.2.158. A solução deve oferecer ferramenta de Portal de Acesso de Usuários que permita que usuários acessem aplicações internas a partir de rede externas, implementando as funcionalidades de Single Sign-on e VPN-SSL, com os seguintes recursos:
- 3.2.158.1. modo “Túnel por aplicação” onde o usuário estabelece túnel somente para o tráfego da aplicação, não sendo permitido outro tipo de tráfego dentro do mesmo túnel;
- 3.2.158.2. modo “Portal” onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;
- 3.2.158.3. modo “Network”, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna;
- 3.2.158.4. Ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeiram autenticação, fazendo cache das credenciais do usuário e utilizar a credencial correta para cada sistema;
- 3.2.159. Deverá ser capaz de autenticar usuários em bases de dados LDAP, Radius, Tacacs+, Kerberos e RSA SecurID;
- 3.2.160. Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware ou one-time passcode (OTP); Deve possuir capacidade para realizar proxy reverso com a finalidade de omitir a URI real, promovendo assim o acesso seguro as aplicações web internas;
- 3.2.161. Deverá prover acesso remoto através de VPN SSL para Microsoft Windows, Linux, dispositivos/ baseados em Android e iOS e MAC OSX;
- 3.2.162. Deve possuir capacidade para realizar verificações e validações no dispositivo do cliente antes de conceder acesso tais como versão do sistema operacional, anti-vírus instalado, certificados digitais instalados na máquina, firewall ativado;
- 3.2.163. Melhora da disponibilidade das aplicações através do balanceamento da entrada de tráfego deve possuir, ao menos, as seguintes características:
- 3.2.163.1.1. DNS autoritativo;
- 3.2.163.1.2. DNS secundário;
- 3.2.163.1.3. DNS resolver;
- 3.2.163.1.4. DNS cache;
- 3.2.163.1.5. Balanceamento de DNS servers;
- 3.2.163.1.6. DNSSec;
- 3.2.164. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;

- 3.2.165. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;
- 3.2.166. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT
- 3.2.167. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;
- 3.2.168. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;
- 3.2.169. Deve prover as respostas a queries DNS da própria RAM CACHE
- 3.2.170. A solução deve ser capaz de realizar IP Anycast;
- 3.2.171. A solução deve ser capaz de realizar DNSSEC, independente da estrutura dos servidores DNS em uso
- 3.2.172. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;
- 3.2.173. Suportar pelo menos os seguintes algoritmos de balanceamento:
 - 3.2.173.1. Round Robin;
 - 3.2.173.2. Global Availability;
 - 3.2.173.3. Ratio;
 - 3.2.173.4. LDNS Persist;
 - 3.2.173.5. Geografia;
 - 3.2.173.6. Disponibilidade da Aplicação;
 - 3.2.173.7. Capacidade do Virtual Server;
 - 3.2.173.8. Least Connections;
 - 3.2.173.9. Pacotes por segundo;
 - 3.2.173.10. Round trip time;
 - 3.2.173.11. Hops;
 - 3.2.173.12. Packet Completion Rate;
 - 3.2.173.13. QoS definido pelo usuário;
 - 3.2.173.14. Kilobytes per Second;
- 3.2.174. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);
- 3.2.175. A solução deve suportar edns-client-subnet (ECS) para tanto responder requisições de clientes ou encaminhar requisições de clientes (screening).
- 3.2.176. Baseado no ECS DNS deve ser possível preservar o endereço IP da subnet do cliente ao invés do LDNS para tomar decisões .
- 3.2.177. A solução deve funcionar pelo menos das seguintes formas:
 - 3.2.177.1. Usar o ECS para tomar decisões baseado em topologia (Subnets)
 - 3.2.177.2. Injetar o ECS (proxy requests) para outros servidores DNS
- 3.2.178. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver (suporte ECS).
- 3.2.179. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;
- 3.2.180. Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);
- 3.2.181. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;
- 3.2.182. Permitir o balanceamento de aplicações em um pool de servidores, independentemente do hardware, sistema operacional e tipo de aplicação;
- 3.2.183. Suportar os seguintes métodos de balanceamento:
 - 3.2.183.1. Round Robin;
 - 3.2.183.2. Least Connection;
 - 3.2.183.3. Por peso.
 - 3.2.183.4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;
 - 3.2.183.5. Weighted Percentage dinâmico (baseado no número de conexões);
 - 3.2.183.6. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;
- 3.2.184. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web.
- 3.2.185. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
 - 3.2.185.1. Por cookie;
 - 3.2.185.2. Endereço de origem;
 - 3.2.185.3. Sessão SSL;
 - 3.2.185.4. Análise da URL acessada;
 - 3.2.185.5. Através de qualquer parâmetro do cabeçalho HTTP;
 - 3.2.185.6. Através da análise do MS Terminal Services Session (MSRDP)

- 3.2.185.7. Através da análise do SIP Call ID ou Source IP;
- 3.2.185.8. Através da análise de qualquer informação da porção de dados (camada 7);
- 3.2.186. O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:
- 3.2.186.1. ICMP, TCP, HTTP, HTTPS;
- 3.2.186.2. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;
- 3.2.187. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor;
- 3.2.188. Realizar Network Address Translation (NAT);
- 3.2.189. Realizar proteção contra syn flood;
- 3.2.190. Realizar as proteções de cabeçalho: X-Frame-Options, X-XSS-Protection, X-Content-Type-Options;
- 3.2.191. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;
- 3.2.192. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.
- 3.2.192.1. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.
- 3.2.192.2. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.
- 3.2.193. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço
- 3.2.194. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;
- 3.2.195. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;
- 3.2.196. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;
- 3.2.197. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;
- 3.2.198. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico;
- 3.2.199. Realizar Network Address Translation (NAT);
- 3.2.200. Realizar Proteção contra Denial of Service (DoS);
- 3.2.201. Realizar Proteção contra Syn flood;
- 3.2.202. Realizar Limpeza de cabeçalho HTTP;
- 3.2.203. Deve possuir suporte a Link Layer Discovery Protocol (LLDP);
- 3.2.204. Deve ser possível enviar, pelo menos, as seguintes informações via LLDP:
- 3.2.205. Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size;
- 3.2.206. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;
- 3.2.207. Deve ser capaz de realizar DHCP relay;
- 3.2.208. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:
- 3.2.208.1. Tempo de resposta da aplicação;
- 3.2.208.2. Latência;
- 3.2.208.3. Conexões para conjunto de servidores, servidores individuais;
- 3.2.208.4. Por URL;
- 3.2.208.5. A solução deve ter suporte a TLS 1.3.

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANT.
3	CAPACIDADE ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB	UN	2

3.3.1. Pacote de Capacidade Adicional, deverá entregar um upgrade de licença para expansão do Throughput da solução do ITEM 1 de, no mínimo, de 3 GBPS.

3.3.2. SUPORTE E GARANTIA;

a) A(s) licença(s) deverá(ão) ser acompanhada(s) de Garantia do Fabricante para o período de 60 meses com

suporte, na modalidade 24x7;

b) Os serviços de suporte serão fornecidos conforme ITEM 9.1 deste Termo de Referência

3.3.3. Caso a solução ofertada não utilize esta modalidade de licenciamento ou em que as funcionalidades deste item já estejam contempladas em um dos demais contidos no lote, demonstrados na proposta, o valor do item deverá figurar como R\$ 0,01 (um centavo) e ele não poderá ser adquirido por adesão.

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANT.
4	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	UN	1

Especificação técnica mínima

3.4.1. Serviço de instalação: os serviços de instalação física, lógica serão executados pela CONTRATADA e deverão ser estruturados conforme as fases a seguir.

3.4.1.1. Fase de abertura:

- a.) Validar e Homologar escopo do projeto;
- b) Validar objetivos e premissas do projeto;
- c) Validar riscos e restrições do projeto;
- d) Identificar e validar os requisitos do projeto;
- e) Efetuar o levantamento de informações sobre o ambiente atual, em complementação ao conjunto de informações apresentado nesta especificação técnica;
- f) Efetuar o gerenciamento de mudanças, contemplando análise de riscos de implementação do sistema;
- g) Apresentar o estudo dos riscos envolvidos na migração para o novo sistema a ser implantado.

3.4.1.2. Fase de planejamento:

- a) Elaborar plano de projeto;
- b) Definir as pessoas envolvidas por parte da CONTRATANTE no projeto;
- c) Reunir as equipes da CONTRATADA e CONTRATANTE;
- d) Definir os parâmetros de configuração básicos e avançados a serem implementados;
- e) Apresentar o Mapa de rede contendo a topologia a ser implementada;
- f) Apresentação do cronograma do projeto com os prazos e responsabilidades;
- g) Verificar os pré-requisitos do projeto;
- h) Apresentar plano do projeto para a homologação por parte da CONTRATANTE.

3.4.1.3. Fase de execução: O serviço de instalação consiste na colocação do(s) equipamento(s) em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da CONTRATANTE e deve contemplar, no mínimo, o seguinte:

- a) Deverão ser realizados por conta da contratada o armazenamento, a embalagem, o transporte, a entrega e a instalação de todo e qualquer item do objeto do edital, de tal maneira que a contratada será responsável pela remessa de todos os equipamentos para o(s) endereços informados no Edital, nos quais a solução de segurança será efetivamente implantada.
- b) A CONTRATADA deverá efetuar instalação e configuração realizada de acordo com as recomendações do fabricante (recommended settings);
- c) A CONTRATADA deverá efetuar a instalação do appliance virtual ou físico (conforme item solicitado) na infraestrutura indicada pelo CONTRATANTE, onde a configuração realizada deverá estar em conformidade com as recomendações do fabricante (recommended settings);
- d) Conexão e configuração de todos os equipamentos e/ou componentes da solução da rede do CONTRATANTE, inclusive configuração de VLANs e interfaces virtuais, se for o caso;
- e) Atualização de softwares, firmwares e drivers que compõem a solução;
- f) A CONTRATADA deverá fornecer, quando for o caso, todos os equipamentos, componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes da solução entregue;
- g) Aplicação das licenças necessárias à solução entregue;
- h) Testes da solução, incluindo testes de failover;
- i) Documentação do ambiente configurado e instalado.

3.4.2. Os serviços de instalação e configuração deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante em seus manuais de instalação e configuração ou artigos técnicos.

3.4.3 A solução, deverá ser entregue com todas as funcionalidades, recursos, componentes, acessórios, softwares e licenciamentos necessários ao seu pleno funcionamento.

3.4.4. Todas as informações necessárias à implantação, como topologia de rede, VLANs, endereçamento IP, portas de Switchs que devem ser utilizadas e outras necessárias à perfeita configuração, interligação e funcionamento da solução serão fornecidas pelo CONTRATANTE.

3.4.5. A instalação da solução, incluindo todos os componentes e acessórios, será realizada pela CONTRATADA, com acompanhamento de uma equipe destacada pela CONTRATANTE.

3.4.6. A CONTRATADA deverá providenciar um profissional certificado pelo fabricante na solução para garantir a conformidade da instalação e a configuração dos equipamentos e softwares que compõem a solução.

3.4.7. A instalação, configuração e testes do equipamento deverá ser feita com o acompanhamento de técnicos da CONTRATANTE, visando o repasse de conhecimento e observados os padrões de gerenciamento de manutenção e segurança da CONTRATANTE.

3.4.8. A CONTRATADA deverá efetuar a instalação/configuração conforme a definição da arquitetura de cada sistema, envolvendo pelo menos:

- a) O agrupamento dos "appliances" em configuração do tipo "cluster" do tipo ativo/ativo ou ativo/passivo;
- b) Segmentação das redes por meio do uso de VLANs;
- c) Definição das redes IP a serem empregadas pelos servidores reais (redes de serviço);
- d) A criação de usuários para fins de operação e administração do sistema.
- e) Configuração de alarmes e notificações automatizadas a serem enviadas via protocolos SNMP e/ou SMTP.
- f) Configuração da topologia de conectividade de rede entre o sistema e os ativos de rede em operação nos datacenters do contratante
- g) Instalação, registro e ativação de licenças para todos os equipamentos ofertados, em total conformidade com essa especificação técnica.
- h) Teste e homologação do conjunto de recursos e funcionalidades do sistema implantado.

3.4.9. A critério do CONTRATANTE, os serviços poderão ser executados fora do horário comercial e/ou em finais de semana ou feriados sem custo adicional para o contratante, visando minimizar os transtornos aos usuários devido a uma eventual indisponibilidade dos serviços. Por conseguinte, as atividades que não tenham impacto de indisponibilidade ou que não venham a requerer a parada dos equipamentos poderão ser executadas em horário comercial. Para as atividades que tenham impacto de disponibilidade ou que venham a requerer a parada dos equipamentos deverão ser executadas fora do horário de expediente, inclusive em feriados ou finais de semana, de acordo com o estabelecido entre a CONTRATADA e o CONTRATANTE.

3.4.9.1. Atividades associadas à implantação com a necessidade de interrupção de serviços em produção, deverão ocorrer fora do expediente normal do Tribunal e estarão sujeitas ao planejamento e aprovação prévia da equipe técnica da CONTRATANTE.

3.4.10. O serviço de implantação da solução deverá ser concluído no prazo de, no máximo, 30(trinta) dias, contados a partir da confirmação do recebimento da Ordem de Serviço.

3.4.10.1. Para todos os efeitos, a conclusão dos serviços de instalação e configuração será atestada pela entrega do sistema em pleno funcionamento, incluindo documentação "As Built", contendo planejamento, relatório de instalação, configuração adotada, testes realizados e seus resultados, de acordo com as especificações do(s) fabricante(s) e demais condições estabelecidas nesta especificação técnica.

3.4.11. Características do repasse de conhecimento hands-on: as atividades de instalação deverão ser acompanhadas na modalidade hands-on, devendo a CONTRATADA:

- a) Efetuar o repasse hands-on com carga horária de, no mínimo, 6 (seis) horas para o repasse de conhecimento referente à integração da solução e sua implantação com a transferência das informações básicas de configuração e operação;
- b) O repasse de informações deverá cobrir conhecimentos mínimos necessários para administração, configuração, otimização, resolução de problemas e utilização da solução;
- c) A equipe técnica do Tribunal, responsável pela infraestrutura técnica deverá disponibilizar no mínimo 2(dois) e no máximo 6(seis) técnicos para o acompanhamento das atividades de hands-on.

3.4.11.1. As horas do acompanhamento hands-on deverão ser distribuídas ou organizadas da melhor maneira durante as atividades de instalação/configuração, mediante proposição da equipe técnica do Tribunal, com a anuência da fiscalização do Contrato.

3.4.11.2. Condições de aceitação do repasse hands-on

3.4.11.2.1. Não serão recebidos os serviços de hands-on prestados por profissionais que não estejam hábeis a demonstrar na prática as funcionalidades principais da solução WAF, particularmente, as atividades relacionadas à mudança de configuração e operação da solução.

3.4.11.2.2. A não aceitação do hands-on implicará a não aceitação da entrega definitiva do serviço (ITEM 4).

3.4.11.3. Todas as despesas de instrutor(es), deslocamento de instrutor(es) e demais itens relacionados ao repasse Hands-On, serão de responsabilidade da CONTRATADA.

ITEM	ESPECIFICAÇÃO	UNIDADE	QUANT
------	---------------	---------	-------

		DE MEDIDA	
5	TREINAMENTO ESPECIALIZADO	UN	6
<p>Especificação técnica mínima</p> <p>3.5.1. Trata-se do serviço de treinamento da solução, na modalidade de fornecimento de voucher para treinamento, cujo escopo do treinamento cubra conceitos de configuração, operação, administração, gerência, otimização, resolução de problemas e gestão de todos os componentes da solução de forma que o(s) servidor(es) capacitado(s) possam colocar os equipamentos e softwares em produção, bem como planejar mudanças de configuração no ambiente.</p> <p>3.5.1.a) O treinamento deverá oferecer carga horária total de no mínimo 20(vinte) horas.</p> <p>3.5.1.b) Serão aceitos preferencialmente treinamentos nas modalidades online ao vivo (EAD), podendo os treinamentos online ao vivo serem gravados, a critério da CONTRATANTE.</p> <p>3.5.1.c) A CONTRATADA deve prover capacitação técnica em turma com no mínimo 5 (cinco) e no máximo 8 (oito) participantes.</p> <p>3.5.1.d) Se o treinamento for ofertado na modalidade EAD, deverá respeitar o limite de 4 (quatro) horas por dia.</p> <p>3.5.1.e) O treinamento deverá cobrir conhecimentos necessários para instalação, administração, configuração, gerência, otimização, resolução de problemas e utilização da solução.</p> <p>3.5.2. As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão de exclusiva responsabilidade da CONTRATADA.</p> <p>3.5.3. O treinamento poderá ser composto de mais de 1(um) módulo, que deverão ser discriminados na proposta da licitante.</p> <p>3.5.4. A licitante deverá anexar a grade de treinamentos do fabricante, com a ementa do(s) curso(s), para comprovar que o(s) treinamento(s) ofertados atendem os requisitos indicados no item 3.5.1.e.</p> <p>3.5.5. O Tribunal poderá planejar e escolher quaisquer das datas, ou períodos, dos eventos de capacitação no prazo de validade da ata de registro de preços, a contar da entrega do calendário.</p> <p>3.5.6. O treinamento deverá ser ministrado em data oportuna a ser informada à fiscalização após ou antes da instalação dos equipamentos, ficando a critério da administração e baseando-se no calendário a ser fornecido pela contratada.</p> <p>3.5.7. É permitido à CONTRATADA terceirizar o treinamento a outra que preste serviços de treinamento da solução ofertada, ou ao próprio fabricante, desde que mantidas as demais condições deste documento e permanecendo ela a única responsável pelo atendimento do contratado para todos os fins.</p> <p>3.5.8. O treinamento deverá ser ministrado por profissionais certificados pelo fabricante (com a certificação mais alta do fabricante), cuja comprovação deverá ser encaminhada na assinatura do Contrato.</p> <p>3.5.9. A contratada deverá fornecer material didático individual, na modalidade digital, que abranja todo o conteúdo do(s) curso(s). Todo o material didático oferecido pela Contratada para realização do treinamento, atualizado e poderá estar em inglês ou português.</p> <p>3.5.10. O treinamento deve ser ministrado em português do Brasil. Caso não exista material oficial do produto em língua portuguesa, será aceito material em inglês.</p> <p>3.5.11. O treinamento deverá oferecer acesso a laboratório prático virtual, fornecido pela contratada, para configuração e execução de exercícios práticos.</p> <p>3.5.11.1. No ambiente de treinamento, os servidores indicados pelo CONTRATANTE devem ter acesso em ambiente de laboratório a todos os produtos ofertados (ou similares) para realização da capacitação.</p> <p>3.5.11.2. Após a conclusão da capacitação, o ambiente EAD deverá permanecer disponível ao acesso do aluno por um prazo mínimo de 12(doze) meses, sob demanda do CONTRANTE.</p> <p>3.5.12. A Contratada deverá emitir para o servidor participante, sem ônus para o Tribunal e no prazo máximo de até 10 (dez) dias úteis após o término do treinamento, o certificado de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária. A cópia deste certificado deverá acompanhar a nota fiscal/fatura para o devido pagamento.</p> <p>3.5.13. A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo à contratada informar no certificado a carga horária e assiduidade do servidor.</p> <p>3.5.14. A Contratada deverá aplicar o Formulário de Satisfação, conforme modelo de formulário constante no Anexo III deste Termo de Referência.</p> <p>3.5.14.a) No Formulário, será utilizada escala de até 4 (quatro) pontos para cada quesito do formulário. No mínimo 70% dos participantes deverão atribuir grau igual ou superior a 3 (três), para o item avaliado ser considerado proveitoso.</p> <p>3.5.14.b) O resultado da Avaliação de Instrutor será utilizado como critério de aceitação do treinamento, devendo ser considerado pela amostra de participantes como “proveitoso” para no mínimo 04(quatro) dos 07(sete) itens avaliados;</p>			

- 3.5.14.c) Caso o resultado da Avaliação de Instrutor seja considerado “não proveitoso”, o treinamento fornecido será considerado não aceito;
- 3.5.14.d) Na hipótese de não aceitação, a CONTRATADA deve oferecer outro treinamento, com a mesma carga horária, com outro instrutor, sem qualquer ônus para o CONTRATANTE;
- 3.5.14.e) Na hipótese de o resultado do segundo treinamento ser “não proveitoso”, o objeto será considerado não aceito, aplicando-se as sanções previstas contratualmente.

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANT.
6	SERVIÇO DE OPERAÇÃO ASSISTIDA	UN	1
<p>Especificação técnica mínima</p> <p>3.6.1. Entende-se por Operação Assistida o acompanhamento e monitoramento remoto (não presencial) pela CONTRATADA da solução em produção, durante 10 (dez) dias úteis contínuos, imediatamente após a fase de implantação da solução, visando atender, operar e solucionar todas as dúvidas e problemas que possam ocorrer.</p> <p>3.6.2. A CONTRATADA deverá apoiar o início das atividades técnicas da nova solução, garantindo apoio imediato e acesso rápido às soluções para alterar ou aplicar configurações necessárias ao ajuste, caso necessário, do ambiente de produção.</p> <p>3.6.3. A CONTRATADA deverá manter à disposição da CONTRATANTE, durante o período de operação assistida, pessoal técnico especializado e qualificado para o acompanhamento e verificação do desempenho operacional e eliminação imediata de eventuais falhas detectadas no sistema.</p> <p>3.6.4. A equipe técnica da CONTRATADA, a qual será responsável pela prestação dos serviços de Operação Assistida, deverá possuir certificação pelo fabricante de cada sistema fornecido/implantado.</p> <p>3.6.5. O serviço de Operação Assistida deverá monitorar o ambiente da CONTRATANTE em horário a ser definido pela CONTRATANTE, podendo ser no período matutino, vespertino ou noturno, não excedendo 8h (oito horas) por dia.</p> <p>3.6.6. A contratada deverá propor e tomar todas as ações necessárias para a prevenção da repetição das falhas que ocorrerem durante o período de execução dos serviços de operação assistida.</p> <p>3.6.7. A CONTRATADA deverá realizar os ajustes necessários para assegurar a disponibilidade e desempenho do ambiente, devendo, ao final dos serviços, emitir relatório com os seguintes dados: (i) Uso computacional e de capacidade do ambiente; (ii) Problemas ocorridos durante o período, as soluções adotadas; (iii) Disponibilidade do ambiente.</p>			

4 APRESENTAÇÃO DA PROPOSTA

- 4.1. Somente serão classificadas as propostas cujos produtos/serviços atendam às especificações mínimas descritas neste Termo de Referência;
- 4.2. Nos preços propostos deverão estar inclusos todas as despesas para seu fornecimento, como: transportes, tributos, etc;
- 4.3. A proposta da licitante deverá vir acompanhada de documentação técnica que comprove o atendimento de todos os requisitos deste termo de referência. Para tal, deverá ser indicado na proposta comercial os part number(s) referente(s) (PartNumbers/SKUs) a cada software(s) fornecido(s), licenças de uso e garantia do produto. Adicionalmente, **a licitante deverá indicar, ponto a ponto, qual seção da documentação técnica comprova o atendimento de cada requisito e conformidade do material proposto** com a especificação exigida deste termo de referência, evitando a pura transcrição do disposto neste Termo de Referência para a proposta;
- 4.4. A LICITANTE deverá indicar em sua proposta os fabricantes, modelos e versões de todos os componentes das soluções, incluindo componentes de hardware (se houver) e de software, realizando a indicação de todos os Códigos de Produto. Devem ser entregues prospectos/folders/folhetos com as

características técnicas dos equipamentos, softwares e licenças. Devem ser apresentadas, de forma clara e detalhada, as descrições das soluções com todos os seus componentes (hardware e software), podendo ser complementadas por documentações integrantes da proposta, tais como: brochuras, catálogos, manuais técnicos, manuais de operação, etc. Na especificação técnica devem ser destacados e referenciados pelo licitante os requisitos mínimos exigidos no Termo de Referência, com a indicação do documento e página onde se encontra grifada a comprovação, sob pena de desclassificação;

4.5. A LICITANTE garantirá que o bem, quer seja de sua fabricação ou integralmente ou parcialmente de subfornecedores, estará exatamente de acordo com estas especificações, isentos de defeitos de fabricação, de matéria prima ou mão de obra. Deverá, também, ser informado o prazo de garantia, conforme especificado neste Termo de Referência;

4.6. A proposta deverá possuir validade mínima de 60 (sessenta) dias.

4.7. Os quantitativos e os valores máximos de referência para a licitação são os seguintes:

GRUPO 1 - SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF)				
ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	CATMAT	QTDE.
1	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE VIRTUAL, COM GARANTIA DE 60(SESENTA) MESES.	UN	27464	2
2	FORNECIMENTO DE ?SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE FÍSICO, COM GARANTIA DE 60(SESENTA) MESES.	UN	27464	2
3	CAPACIDADE ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB	UN	27464	2
4	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	UN	20419	1
5	TREINAMENTO ESPECIALIZADO	UN	3840	6
6	SERVIÇO DE OPERAÇÃO ASSISTIDA	UN	20419	1

Tabela 4 - Modelo de proposta - Bens e serviços que compõem a solução

5. ESTRATÉGIA DA CONTRATAÇÃO

5.1 Regime, Tipo e Modalidade da Licitação

- O certame se realizará na forma licitação tradicional, na modalidade PREGÃO ELETRÔNICO SISTEMA DE REGISTRO DE PREÇOS, do tipo MENOR PREÇO GLOBAL.

5.2 Margem de Preferência

- Não Aplicável à Contratação.

5.3. Critérios de Julgamento das Propostas

5.3.1. Durante a apresentação da proposta, a licitante deverá demonstrar que o produto ofertado atende às exigências solicitadas nesta especificação. Para esta comprovação, serão aceitos catálogos, *datasheets*, manuais, sites ou outra documentação oficial onde se possa identificar de maneira inequívoca o modelo de equipamento proposto.

5.3.2. Em caso de dúvidas na comprovação da especificação, poderão ser solicitados por meio de diligência, esclarecimentos sobre a especificação dos produtos cotados pela licitante.

5.3.3. A licitante deverá apresentar declaração de que o produto atende a todas especificações exigidas.

5.4 . Critérios de Qualificação Técnica para a Habilitação

5.4.1. A LICITANTE deverá apresentar pelo menos 01 (um) atestado de capacidade técnica, fornecido (s) por pessoa jurídica de direito público ou privado, que comprove o fornecimento e implantação de solução de Web Application Firewall (WAF) em appliance virtual e físico, a fim de comprovar a aptidão para desempenho de atividade pertinente e compatível com o objeto da licitação.

5.4.2. Os atestados deverão conter as seguintes informações mínimas: nome e cargo da pessoa que os assina, quantitativo associado ao fornecimento, valor e/ou Contrato(s) associado(s) à prestação dos serviços;

5.4.3. A critério do pregoeiro, as licitantes deverão disponibilizar informações adicionais necessárias à comprovação da legitimidade do(s) atestado(s) apresentado(s), inclusive cópia de pelo menos uma nota fiscal do serviço constante no documento apresentado.

5.4.4. Conforme art. 43, §3º da Lei nº 8.666/93, os conteúdos dos atestados/declarações serão objeto de averiguação pelo TRE-PA, mediante diligências.

5.4.5. Ainda, em termos de diligência, o TRE-PA se reserva ao direito de entrar em contato com os gestores do contrato, realizar visita(s) ou reuniões com as entidades emissoras de forma a sanar dúvidas e atestar a veracidade das informações apresentadas. Devido a tal, todas as informações necessárias à comprovação da legitimidade dos atestados solicitados poderão ser solicitadas para averiguação. Quais sejam: cópia do contrato que deu suporte à contratação, Relatórios Técnicos de Controle ou Execução do Contrato, Notas Fiscais, Ordens de Serviço, endereço e telefones dos gestores do contrato e local em que foram prestados os serviços.

5.5. Documentação exigida - fase de assinatura do contrato.

5.5.1. A CONTRATADA deverá apresentar após assinatura do contrato, no prazo de até 10 (dez) dias contados da publicação do extrato do Contrato no Diário Oficial da União, a documentação associadas ao(s) profissional(is) envolvidos e certificações mínimas associadas à execução dos serviços, conforme os itens a seguir.

5.5.2. A licitante contratada deverá apresentar analista (s) integrador (es) – conjunto com um ou mais profissionais, certificados pelo fabricante da solução, que individualmente ou conjuntamente serão responsáveis pelos serviços de implantação e transferência tecnológica.

5.5.3. As certificações profissionais serão auditadas no início dos serviços pela fiscalização do Contrato.

5.5.4. Nos casos da CONTRATADA não apresentar as certificações ou das certificações apresentadas não corresponderem às solicitadas, o CONTRATANTE terá autonomia para solicitar a troca do profissional indicado a qualquer tempo. O TRE-PA não autorizará o início dos serviços enquanto não for apresentado técnico certificado.

5.5.5. Após o recebimento do pedido de instalação, a contratada terá 5 (cinco) dias úteis para informar o técnico que fará a instalação acompanhada da comprovação da certificação exigida.

5.6. Dotação Orçamentária

5.6.1. As despesas para aquisição do objeto deste Termo de Referência correrão por conta do Elemento de Despesa 44.90.52.35 - Equipamentos de Processamento de Dados, correspondente aos exercícios associados à vigência da ata de registro de preços.

5.7 Critérios Sociais e Culturais

5.7.1. Todos os manuais, guias de instruções e ajuda deverão ser disponibilizados preferencialmente para o idioma Português do Brasil - PtBR e fornecidos em meio digital.

5.7.2. O licenciamento e o suporte devem ser prestados preferencialmente no idioma português do Brasil.

5.7.3. Os softwares aplicativos e interface do software devem ter a possibilidade de escolha de idioma pelo usuário. Será admitido o idioma inglês somente quando não existir uma versão no idioma português do Brasil.

5.7.4. Os profissionais da CONTRATADA deverão trajar-se de maneira respeitável e usar linguagem respeitosa e formal no trato com os servidores do órgão, Gestão Contratual e os dirigentes da CONTRATANTE.

5.8 Critérios de Segurança da Informação

5.8.1. Manutenção de Sigilo e Normas de Segurança

- A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.
- O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e Termo de Ciência, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos ANEXOS I - TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO e ANEXO II - TERMO DE CIÊNCIA.

5.9 Possibilidade de Adesão à Ata de Registro de Preços por outros órgãos

5.9.1. Por não haver excepcionalidade, conforme orientações dos Acórdãos TCU nº 757/2015- Plenário e 2037/2019 – Plenário, o objeto da ARP não possibilitará adesões de outros órgãos da Administração Pública, com exceção dos Tribunais Regionais Eleitorais que figuram como partícipes deste Edital.

6. DEFINIÇÃO DAS OBRIGAÇÕES CONTRATUAIS

6.1. Definição das obrigações da contratante

6.1.1. A CONTRATANTE obriga-se a promover, por intermédio de Comissão ou servidor designado na forma do art. 67 da Lei n.º 8.666/93, o acompanhamento e a fiscalização da execução do objeto do contrato, conforme a seguir:

6.1.2. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

6.1.3. Anotar em registro próprio os defeitos detectados e comunicando as ocorrências de quaisquer fatos que, a seu critério, exijam o reparo ou substituição dos bens por parte da CONTRATADA.

6.1.4. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

6.1.5. A existência de fiscalização da CONTRATANTE de modo algum atenua ou exime a responsabilidade da CONTRATADA por qualquer vício ou defeito presente nos bens fornecidos.

6.1.6. Abrir e acompanhar os chamados técnicos à contratada, elaborando relatórios mensais, constando as conformidades e desconformidades dos serviços prestados;

6.1.7. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

6.1.8. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através de comissão/servidor especialmente designado;

6.1.9. Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

6.1.10. A Administração não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

6.2. Definição das obrigações da contratada

6.2.1. A CONTRATADA obriga-se a fornecer o material obedecendo rigorosamente às especificações discriminadas neste Termo de Referência.

6.2.2. A CONTRATADA obriga-se, ainda, a:

a) Manter, durante o fornecimento, todas as condições de habilitação e qualificação exigidas neste Termo de Referência;

b) Não transferir a outrem, no todo ou em parte, o objeto do contrato a ser firmado

6.2.3. A CONTRATADA deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

a) Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo e prazo de garantia;

b) Atender aos chamados técnicos no prazo estipulado pela contratante;

c) Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

d) Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência (item 9.2.3), o objeto com avarias ou defeitos;

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

f) Responsabilizar-se integralmente pelo fiel cumprimento do objeto contratado, prestando todos os esclarecimentos que forem solicitados pela CONTRATANTE, cujas reclamações se obriga a atender.

7. EXECUÇÃO DO CONTRATO

7.1 Prazo de entrega

7.1.1. A entrega de equipamentos, licenças e conclusão de serviços devem obedecer os seguintes prazos:

7.1.1.1. ITEM 1: prazo de entrega de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Fornecimento.

7.1.1.2. ITEM 2: prazo de entrega de, no máximo, 60 (sessenta) dias, contados a partir da confirmação do recebimento da Ordem de Fornecimento.

7.1.1.3. ITEM 3: prazo de entrega de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Fornecimento.

7.1.1.4. ITEM 4: prazo de execução de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Serviço.

7.1.1.5. ITEM 5. prazo de execução de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Serviço.

7.1.1.6. ITEM 6. prazo de execução de, no máximo, 10 (dez) dias úteis contínuos, imediatamente após a fase de implantação da solução.

7.1.2. Os prazos de entrega, substituição e reposição admitem prorrogação, mantidas as demais cláusulas da contratação e da nota de empenho que não sofrerem influência dessa prorrogação, sendo assegurada a manutenção do equilíbrio econômico-financeiro da contratação, desde que ocorra um dos motivos

previstos nos incisos I a VI do § 1º do Art. 57 da Lei n. 8.666/93, devendo ser requerida por escrito, justificadamente, e apresentada até o último dia do referido prazo.

7.2 Local de execução/entrega

7.2.1. Tribunal Regional Eleitoral do Pará (Sede), rua João Diogo 288, Campina , Belém- PA- CEP 66015-902, Anexo I, Seção de Serviços de Redes (SSR).

7.3 Condições gerais do fornecimento

7.3.1. A entrega dos materiais deverá efetuar-se no local de entrega designado no item 7.2.1, de segunda a sexta-feira, no horário das 08 às 15h;

7.3.2. Todos os custos, ônus, e obrigações e encargos deverão ser arcados pela contratada para entrega dos equipamentos nos endereços descritos neste TR.

7.3.3. Havendo alteração no endereço de entrega, sem alteração do município, o mesmo será disponibilizado por ocasião da entrega da Nota de Empenho;

7.3.4. Os produtos definidos neste Termo deverão ser novos e sem utilização anterior, originais e de boa qualidade, livres de defeitos, imperfeições e outros vícios que impeçam ou reduzam a usabilidade, observando rigorosamente as características especificadas, devendo ser apresentados nas embalagens originais dos fabricantes, adequadas para proteger seu conteúdo contra danos durante o transporte até o local de entrega;

7.3.5. O fornecedor deverá apresentar a garantia correspondente a cada item, a contar da data de aceite efetuada pelo TRE-PA.

7.3.6. Comunicar o TRE-PA, com antecedência razoável, a entrega e execução de serviços associados ao item 7 do Termo de Referência, com o propósito de possibilitar agendamento e organização pela unidade responsável pela fiscalização destas atividades, evitando-se o comprometimento do regular funcionamento dos serviços do órgão.

8. FORMA DE PAGAMENTO

8.1. A CONTRATADA deverá apresentar ao Tribunal Regional Eleitoral do Pará Nota Fiscal/Fatura da própria empresa, na forma impressa ou eletrônica, a qual será encaminhada para pagamento após o recebimento e o aceite definitivo de material e serviços associados ao objeto. A Nota Fiscal poderá ser encaminhada por e-mail para o endereço eletrônico a ser informado oportunamente pela fiscalização.

8.1.1. Se optante pelo Simples Nacional, deverá ser apresentada a declaração de que trata o art. 6º da Instrução Normativa nº 1234/2012, em meio físico ou eletrônico assinado por certificação digital (não será aceite simples cópia digitalizada).

8.2. O pagamento será efetuado através de Ordem Bancária, mediante depósito na conta corrente da CONTRATADA, até o 10º (décimo) dia útil da data da liquidação da despesa, observado o estabelecido no art. 5º da Lei nº 8.666/93, e desde que não ocorra fator impeditivo provocado pela CONTRATADA.

8.3. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária de pagamento.

8.4. No caso do valor do pagamento não ultrapassar o limite de que trata o inciso II do art. 24, da Lei n.º 8.666/93, o mesmo deverá ser efetuado no prazo de até 5 (cinco) dias úteis, nas condições referidas acima.

8.5. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento dos preços ou correção monetária.

9. GESTÃO DO CONTRATO

9.1. DA GARANTIA E DO SUPORTE TÉCNICO

9.1.1 A garantia refere-se ao período oficial de suporte da solução, fornecido por seu fabricante, compreendendo o fornecimento de atualizações e correções durante todo o ciclo de vida da versão fornecida do sistema operacional.

9.1.1.a. A vigência da garantia começará a contar a partir do recebimento definitivo pela Comissão indicada pelo Gestor do Contrato.

9.1.2.b. Durante a vigência da garantia, o fornecedor deverá comunicar ao CONTRATANTE eventual alteração do número telefônico ou do e-mail para abertura de chamados.

9.1.2. A Contratada deverá fornecer garantia técnica de pelo menos 60 (sessenta) meses para a solução, contados a partir da data de emissão do Termo de Recebimento Definitivo relativo à fase de instalação;

9.1.3. Os serviços de garantia técnica englobam todos os elementos de hardware e software da solução, incluindo a prestação de serviços de suporte técnico, assistência corretiva e atualização tecnológica, compreendendo a substituição de peças, componentes, acessórios e aplicativos que apresentem defeito, ou precisem ser atualizados durante este período, sem qualquer ônus adicional para o CONTRATANTE, obrigando-se a Contratada a manter os equipamentos e aplicativos permanentemente em perfeitas condições de funcionamento para a finalidade a que se destinam;

9.1.4. A garantia técnica compreenderá todas as funcionalidades da solução ofertada, tanto as descritas no Termo de Referência quanto as contempladas nos manuais e demais documentos técnicos, incluindo a atualização de versões de software;

9.1.5. Qualquer software ou equipamento com hardware defeituoso, peças quebradas, com defeito ou gastas pelo uso normal deverá ser substituído por outro de mesma marca e modelo e com as mesmas características técnicas ou superiores, novo e de primeiro uso, no prazo de 48 (quarenta e oito) horas a partir de notificação do CONTRATANTE;

9.1.6. A Contratada deverá apresentar no protocolo do CONTRATANTE, antes do início da vigência do serviço de garantia técnica, todos os dados necessários para o registro de chamados técnicos na Central de Atendimento da Contratada, tais como, e-mail, números de telefone e fax, etc;

9.1.7. Suporte Técnico durante o período de Garantia Técnica:

9.1.7.a. Durante o período de garantia técnica de 60 (sessenta) meses, a partir do recebimento definitivo da instalação, a Contratada deverá garantir o funcionamento de toda a solução, fornecer atualizações, prestar suporte técnico e atender aos chamados técnicos para manutenção;

9.1.7.b. A Contratada deverá comunicar formalmente ao Gestor do Contrato a disponibilidade de novas versões e releases das licenças de software e firmwares, reservando-se, à equipe técnica do CONTRATANTE, o direito de exigir a atualização sem que isso implique acréscimo aos preços contratados;

9.1.7.c. A manutenção corretiva será realizada em período integral, 7 (sete) dias por semana e 24 (vinte e quatro) horas por dia, após solicitação do CONTRATANTE;

9.1.8. A contratada deverá entregar no protocolo do CONTRATANTE, mensalmente, até o 5º (quinto) dia útil do mês subsequente, para fins de controle, Relatório Gerencial dos Serviços (RGS) realizado no mês anterior. Deverão constar, no mínimo, as seguintes informações:

9.1.8.a. Relação de todos os chamados técnicos ocorridos no mês anterior, incluindo data e hora do início e término do suporte; identificação do problema; criticidades; providências adotadas para o diagnóstico, solução provisória e solução definitiva; data e hora do início e término da solução definitiva; identificação do técnico do CONTRATANTE que solicitou e validou o chamado; identificação do técnico da Contratada responsável pela execução do chamado, bem como outras informações pertinentes;

9.1.8.b. Cada chamado técnico aberto será avaliado individualmente pelo Gestor do Contrato;

9.1.8.c. O serviço será considerado recebido pelo Gestor do Contrato quando do fechamento de cada chamado, desde que não reapareçam posteriormente ao fechamento inconformidades técnicas comprovadamente relacionadas ao chamado recebido;

9.1.8.d. O Gestor do Contrato emitirá a recusa em caso de verificação de impropriedades ou erros impeditivos de recebimento do serviço prestado. A Contratada deverá promover as correções necessárias, conforme diretrizes a serem estabelecidas pelo Gestor do Contrato, sem prejuízo de aplicação de penalidades previstas.

9.1.9. A Contratada deverá fornecer versão atualizada do manual e demais documentos técnicos sempre que houver atualização nos manuais, nos softwares ou nos equipamentos da solução.

9.1.10. A CONTRATANTE poderá realizar a aplicação de pacotes de correção e migração de versões e releases das licenças de software, quando lhe for conveniente, cabendo à Contratada orientar e colocar à disposição um técnico para contato em caso de dúvidas ou falhas. A CONTRATANTE reserva-se o direito de proceder a outras configurações, instalações ou conexões nos equipamentos, desde que tal iniciativa não implique danos físicos e lógicos aos equipamentos, sem que isto possa ser usado como pretexto pela

Contratada para se desobrigar do suporte da solução.

9.1.11. A Contratada deverá garantir pleno funcionamento dos equipamentos e softwares, bem como atualizações, responsabilizando-se por qualquer componente adicional que for identificado após a contratação, seja por motivos de interoperabilidade, compatibilidade ou quaisquer outros motivos que impeçam o funcionamento efetivo da solução contratada.

9.1.12. A Contratada deverá dispor de serviço de esclarecimento de dúvidas relativas à utilização dos equipamentos e de abertura de chamado técnico por e-mail ou por telefone 0800 (gratuito), ou telefone local em Brasília por todo o período da garantia técnica.

9.1.13. A Contratada deverá garantir, sem quaisquer custos adicionais, as atualizações havidas nos equipamentos nas versões de software e firmware, inclusive releases, pelo prazo de vigência da garantia;

9.1.14. O serviço de garantia técnica deverá permitir o acesso do CONTRATANTE à base de dados de conhecimento do fabricante dos equipamentos, provendo informações, assistência e orientação para diagnósticos, avaliações e resolução de problemas, características dos produtos e demais atividades relacionadas à correta operação e funcionamento dos equipamentos.

9.1.15. As atualizações e correções (patches) do software e firmwares deverão estar disponibilizados via WEB ou fornecidas em mídia (CD ou DVD), quando desta forma forem solicitadas.

9.1.16. Quando a garantia técnica for acionada, o atendimento deverá ser iniciado imediatamente, independente do meio utilizado. A cada abertura de chamado, a Contratada deverá fornecer ao CONTRATANTE um código identificador único para acompanhamento.

9.1.17. A Contratada deverá conceder acesso ao CONTRATANTE ao controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do Gestor do Contrato.

9.2 Do Recebimento Provisório e Definitivo

9.2.1. A CONTRATANTE efetuará o recebimento do objeto contratado, provisoriamente, para efeito de posterior verificação da conformidade do objeto com a especificação, e definitivamente, após a verificação da qualidade e quantidade do objeto e consequente aceitação.

9.2.2. Em caso de rejeição total/parcial do objeto contratado, correção, substituição ou demais hipóteses de descumprimento de outras obrigações contratuais, avaliadas na etapa de recebimento, sujeitará a LICITANTE VENCEDORA à aplicação das sanções administrativas cabíveis.

9.2.3. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias corridos, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

9.3. Termo de recebimento provisório

9.3.1. O CONTRATANTE receberá provisoriamente o objeto contratado, mediante emissão de termo circunstanciado assinado pelas partes, em até 5 (cinco) dias após a entrega do objeto.

9.3.2. O recebimento provisório caberá ao agente fiscalizador especialmente designado para acompanhamento e fiscalização do contrato decorrente desta proposição.

9.3.3. A fiscalização do contrato procederá a observação da qualidade do objeto, registrando a data de entrega dos materiais e a data de emissão do termo de recebimento provisório, bem como anotar quaisquer ocorrências que impactem na avaliação da qualidade do fornecimento pela LICITANTE VENCEDORA.

9.4. Termo de recebimento definitivo

9.4.1. Os representantes da administração deverão conferir a qualidade e especificações funcionais dos equipamentos entregues e confrontá-las com as exigências editalícias, promoverem testes de desempenho (se for o caso), verificar licenças, registrar a data de entrega, emitir o recibo e o termo de recebimento definitivo, bem como registrar quaisquer ocorrências que impactem na avaliação da qualidade do fornecimento pela LICITANTE VENCEDORA.

9.4.2. O recebimento definitivo caberá ao agente fiscalizador especialmente designado para acompanhamento e fiscalização do contrato decorrente desta proposição.

9.4.3. O objeto contratado será rejeitado caso esteja em desacordo com as especificações constantes deste Termo de Referência, devendo a CONTRATANTE apontar por escrito esta ocorrência, onde detalhou as razões para deixar de emitir o termo de recebimento definitivo e indicará as falhas e pendências verificadas.

9.4.4. O recebimento definitivo do objeto não exclui nem reduz a responsabilidade da LICITANTE VENCEDORA com relação ao funcionamento e configuração divergente do especificado, durante todo o seu período de garantia.

9.4.5. Ficam designados para compor a comissão que efetuará o recebimento definitivo o agente fiscalizador e o gestor do contrato, bem como seus respectivos substitutos.

9.4 Sanções Administrativas

9.5.1. Ficará impedida de licitar e de contratar com a União e será descredenciada no SICAF, pelo prazo de até cinco anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantido o direito à ampla defesa, a licitante que, convocada dentro do prazo de validade de sua proposta:

- a) Deixar de entregar a documentação exigida no Edital;
- b) Não assinar a Ata de Registro de Preços ou o contrato e/ou não receber a Ordem de Fornecimento e/ou de Serviço;
- c) Apresentar documento falso ou fizer declaração falsa;
- d) Causar atraso execução do objeto deste Pregão;
- e) Não manter a proposta, injustificadamente;
- f) Falhar ou fraudar na execução do contrato;
- g) Comportar-se de modo inidôneo;
- h) Cometer fraude fiscal.

9.5.2. Sem prejuízo das demais sanções previstas no art. 87 da Lei nº 8.666/93, pelo atraso injustificado e inexecução total ou parcial do objeto deste Pregão, a Administração do Tribunal Regional Eleitoral do Pará, poderá, garantida a defesa prévia, aplicar à licitante vencedora as seguintes sanções:

- a) Advertência, nas hipóteses de faltas leves, assim entendidas aquelas que não acarretem prejuízos para o TRE/PA;
- b) Multa compensatória de até 10% (dez por cento) sobre o valor global da Ata de Registro de Preços, na hipótese de recusa em assinar a Ata de Registro de Preços ou do contrato, na hipótese de recusa em assinar o instrumento de contrato;
- c) Multa compensatória de até 10% (dez por cento) sobre o valor global do respectivo material, na hipótese de recusa em receber a Ordem de Fornecimento e/ou de Serviço;
- d) Multa compensatória de até 10% (dez por cento) sobre o valor global do respectivo material, na hipótese de inexecução parcial ou total da obrigação.

9.5.3. Pelo atraso injustificado na execução do contrato, a CONTRATANTE deverá, garantida a defesa prévia, aplicar à licitante vencedora multa moratória de 0,2% (dois décimos por cento) por dia de atraso na entrega do material e/ou conclusão do serviço contratado, tomando por base o valor global do respectivo material, limitado a 10% (dez por cento).

9.5.3.1. O atraso injustificado na execução do contrato por período superior a 30 (trinta) dias, bem como deixar de manter todas as condições de habilitação, poderá ensejar a rescisão do contrato.

ANEXO I

TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

A Sociedade Empresária _____, CNPJ _____, por intermédio de seu representante legal abaixo assinado, _____, CPF _____

, doravante designados simplesmente CONTRATADA e RESPONSÁVEL, se comprometem, por intermédio do presente TERMO DE COMPROMISSO, a não divulgar sem autorização, quaisquer Informações Confidenciais (conforme definido abaixo) em relação ao Projeto de “Contratação de solução de *Web Application Firewall* (WAF)”, e de propriedade do Tribunal Regional Eleitoral do Pará, CNPJ nº 05.703.755/0001-76, doravante designado TRE-PA, em conformidade com as seguintes cláusulas e condições:

1. Por este instrumento, a Contratada declara estar apta a aceitar e receber INFORMAÇÕES com respeito ao parque tecnológico do TRE-PA, comprometendo-se a manter absoluta confidencialidade destas INFORMAÇÕES, independente de solicitação expressa neste sentido pelo TRE-PA ou quaisquer de seus representantes;
2. As INFORMAÇÕES abrangidas por este termo são de natureza técnica, operacional, comercial, jurídica e financeira expressas de forma escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, ficando expressamente vedada sua divulgação a terceiros, a qualquer título;
3. As partes deverão restringir a divulgação das INFORMAÇÕES para o pessoal que estiverem diretamente envolvidos na sua utilização em razão do fornecimento das INFORMAÇÕES e da elaboração do serviço a ser fornecido, ficando vedado o intercâmbio destas INFORMAÇÕES com terceiros que não estejam diretamente envolvidos com a prestação dos serviços;
4. A CONTRATADA obriga-se a informar imediatamente o TRE-PA qualquer violação das regras de sigilo que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço;
5. A CONTRATADA deverá prestar obediência às políticas de segurança da informação vigentes no Tribunal Regional Eleitoral do Pará ou que poderão ser instituídas durante a vigência do contrato;
6. A não observância de quaisquer das disposições estabelecidas neste instrumento sujeitará a CONTRATADA aos procedimentos judiciais cabíveis relativos a perdas e danos que possam advir ao TRE-PA e aos seus usuários;
7. O descumprimento de quaisquer das cláusulas do presente Termo acarretará a responsabilidade civil e criminal de acordo com as leis aplicáveis dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

Gestor do Contrato do TRE-PA: _____

Representante da Contratada: _____

Local, UF, de de

ANEXO II TERMO DE CIÊNCIA

IDENTIFICAÇÃO DO CONTRATO

CONTRATO Nº:

OBJETO: “Aquisição de solução de *Web Application Firewall* (WAF) e balanceamento de carga, incluindo prestação de serviços de instalação e configuração, com garantia técnica de 60 (sessenta) meses”

Contratada:

CNPJ:

Representante da Contratada:

CPF:

Pelo presente instrumento, o(s) funcionário(s) abaixo qualificado(s) e assinado(s) declara(m):

- Ter plena ciência e conhecimento do Termo de Compromisso e Manutenção de Sigilo firmado pela CONTRATADA;
- Ter conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo que deverá ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato Administrativo;
- Comprometer-se a guardar sigilo necessário sobre todas as informações que eventualmente venha(m) a tomar conhecimento;
- Comprometer-se a prestar obediência às políticas de segurança da informação vigentes no Tribunal Regional Eleitoral do Pará ou que poderão ser instituídas durante a vigência do contrato.

IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)

Nome: CPF: _____

Função/Cargo: _____

Assinatura: _____

Nome: CPF: _____

Função/Cargo: _____

Assinatura: _____

Local, UF, de de .

ANEXO III
AValiação DO ITEM 5 - TREINAMENTO ESPECIALIZADO

AValiação DE REAÇÃO

Curso:
Promotor:
Período:
Carga Horária:
Instrutor:
Objetivo:

Para que possamos avaliar a qualidade do treinamento, assinale com um (X) na nota que melhor expressa sua opinião de acordo com a escala abaixo:

Grau de satisfação	Não atendeu	Atendeu parcialmente	Atendeu plenamente	Superou
Nota	1	2	3	4

I- PROMOTOR DO EVENTO	NOTA			
ITEM	1	2	3	4
1- Quanto à organização do evento				

2- Quanto à adequação das instalações				
3- Quanto à adequação dos recursos audiovisuais				
4- Quanto à qualidade do material didático				
II- CONTEÚDO PROGRAMÁTICO	NOTA			
ITEM	1	2	3	4
1- Quanto ao cumprimento do conteúdo programático				
2- Quanto ao detalhamento na abordagem dos tópicos				
3- Quanto à adequação da carga horária				
4- Quanto a adequação do conteúdo a sua necessidade de conhecimento				
III- INSTRUTOR	NOTA			
ITEM	1	2	3	4
1- Quanto ao domínio do assunto				
2- Quanto à relevância e atualidade dos conhecimentos difundidos				
3- Quanto à promoção de um ambiente favorável à aprendizagem				
4- Quanto à clareza e objetividade nas exposições				
5- Quanto à objetividade na administração do tempo				
6 – Quanto ao incentivo à participação da turma				
7 – Quanto à disponibilidade para o atendimento e o apoio aos alunos				
IV- APROVEITAMENTO	NOTA			
ITEM	1	2	3	4
1- Quanto à assimilação do conteúdo				
2- Quanto à adequação do conteúdo ao objetivo proposto por sua unidade de lotação				
V- COMENTÁRIOS E SUGESTÕES:				

Modelo de formulário - SGP/CODES/Seção de Treinamento e Desenvolvimento



Documento assinado eletronicamente por **ANGELA FIGUEIREDO DA SILVA MERGULHÃO, Coordenadora**, em 19/04/2022, às 14:10, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ANTONIO EDIVALDO DE OLIVEIRA GASPAR, Coordenador**, em 19/04/2022, às 14:17, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **EMERSON DIAS DA SILVA, Chefe de Seção**, em 20/04/2022, às 09:09, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pa.jus.br/sei/controlador_externo.php?



acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1496398** e o código CRC **75B969CC**.

Assinatura

0008981-46.2021.6.14.8000 1496398v178