ESTUDOS PRELIMINARES

I – ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1 ESPECIFICAÇÃO DOS REQUISITOS

1.1 DE NEGÓCIO

1.1.1 A solução deverá:

1.1.1.1 No quesito segurança, fornecer uma camada adicional de defesa, protegendo os servidores que hospedam aplicações *Web*, e executar funções de segurança de proteção dos servidores internos contra-ataques por usuários da Internet.

1.1.1.2 No quesito performance, melhorar o acesso às aplicações dos sistemas judiciários, através do balanceamento de carga.

1.1.1.3 Ampliar o controle de perímetro, por meio da inspeção e análise contínuo de tráfego das aplicações.

1.1.1.4 Aprimorar os mecanismos de monitoramento e detecção de ataques.

1.1.1.5 Proporcionar a prevenção e mitigação de ameaças cibernéticas.

1.1.1.6 Contribuir para a redução da superfície de ataques cibernéticos da Justiça Eleitoral.

1.1.1.7 Possuir gerenciamento e armazenamento dos dados na rede local do Tribunal, com *appliances* próprios localizados e instalados na infraestrutura do cliente (*on-premise*).

1.1.1.8 Ser licenciada para uso perpétuo.

1.1.1.8.1 As funcionalidades da solução deverão 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.

1.1.1.9 Poder ser ofertada na modalidade de *Appliance* Físico ou *Appliance* Virtual.

1.1.1.10 Na contratação, deverá fornecer implantação da solução no ambiente do Tribunal e treinamento EAD.

1.1.2 Atualmente existe a necessidade de aquisição de uma solução específica para atender a nossa demanda, conforme abaixo:

Item	Descrição	Tipo
1	*Cluster*/Solução de proteção camada 7 para Aplicações *Web, Firewall (WAF),* do tipo *Appliance* Físico ou Virtual	*Cluster* de proteção (02 *appliances*) das aplicações *WEB* hospedadas no ambiente de produção (*Data Center*) do Tribunal, visando mitigar os riscos de ataque cibernético
2	Implantação e repasse de conhecimento *HANDS-ON*	Implantação da solução, incluindo instalação e configuração no ambiente do Tribunal e repasse técnico-operacional básico da solução
3	Treinamento Especializado	Capacitação da equipe técnica (até 06 servidores) para administração da solução, por meio de treinamento

1.2 DE CAPACITAÇÃO

1.2.1 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.

1.2.1.1 O treinamento deverá oferecer carga horária total de no mínimo 20 (vinte) horas.

1.2.1.2 Serão aceitos apenas treinamentos nas modalidades *online* ao vivo (EAD), podendo os treinamentos *online* ao vivo serem gravados, a critério do TRE/RN.

1.2.1.3 A fornecedora da solução deve prover capacitação técnica em turma com no mínimo 5 (cinco) e no máximo 08 (oito) participantes.

1.2.1.4 Se o treinamento for ofertado na modalidade EAD, deverá respeitar o limite de 04 (quatro) horas por dia.

1.2.1.5 O treinamento deverá cobrir conhecimentos necessários para instalação, administração, configuração, gerência, otimização, resolução de problemas e utilização da solução.

1.2.2 As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão de exclusiva responsabilidade da fornecedora da solução.

1.2.3 O treinamento poderá ser composto de mais de 01 (um) módulo, que deverão ser discriminados na proposta da licitante.

1.2.4 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 (e) anterior.

1.2.5 O Tribunal poderá planejar e escolher qualquer das datas, ou períodos, dos eventos de capacitação no prazo de validade da ata de registro de preços, a contar da entrega do calendário.

1.2.6 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 fornecedora da solução.

1.2.7 É permitido à fornecedora da solução 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.

1.2.8 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.

1.2.9 A fornecedora da solução deverá fornecer material didático individual, na modalidade digital, que abranja todo o conteúdo do(s) curso(s).

1.2.9.1 Todo o material didático oferecido pela Contratada para realização do treinamento, atualizado e poderá estar em inglês ou português.

1.2.10 O treinamento deve ser ministrado em português do Brasil.

1.2.10.1 Caso não exista material oficial do produto em língua portuguesa, será aceito material em inglês.

1.2.11 O treinamento deverá oferecer acesso a laboratório prático virtual, fornecido pela fornecedora da solução, para configuração e execução de exercícios práticos.

1.2.11.1 No ambiente de treinamento, os servidores indicados pelo TRE/RN devem ter acesso em ambiente de laboratório a todos os produtos ofertados (ou similares) para realização da capacitação.

1.2.11.2 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 TRE/RN.

1.2.12 A fornecedora da solução 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.

1.2.12.1 A cópia deste certificado deverá acompanhar a nota fiscal/fatura para o devido pagamento.

1.2.13 A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo a fornecedora da solução informar no certificado a carga horária e assiduidade do servidor.

1.3 LEGAIS

1.3.1 A contratação obedecerá às regras gerais de fornecimento ao Poder Público, inexistindo requisitos legais específicos para essa contratação.

1.3.2 A fornecedora da solução deve observar o cumprimento de todas as leis e normas aplicáveis ao OBJETO, em especial atenção àquelas relacionadas ao pagamento das obrigações empresariais relacionadas aos encargos fiscais, trabalhistas e previdenciários.

1.3.3 Outras Referências:

1.3.3.1 Resolução CNJ N° 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).

1.3.3.2 Resolução CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

1.3.3.3 Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

1.3.3.4 LGPD – Lei Geral de Proteção de Dados (Lei n° 13.709/2018) e Marco Civil da Internet Lei no 12.965/2014).

1.3.3.5 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.

1.3.3.6 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.

1.3.3.7 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.

1.3.3.8 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.

1.4 MANUTENÇÃO

1.4.1 Suporte técnico deverá estar disponível durante a vigência de uso da licença.

1.4.2 Atualizações da solução deverão estar disponíveis durante a vigência de uso da licença.

1.4.3 A fornecedora da solução 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.

1.4.4 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 TRE/RN, obrigando-se a fornecedora da solução a manter os equipamentos e aplicativos permanentemente em perfeitas condições de funcionamento para a finalidade a que se destinam.

1.5 TEMPORAIS

1.5.1 A fornecedora da solução terá até **05 (cinco) dias** contados após a formalização da contratação para fornecer os *softwares* ou as subscrições contratadas.

1.6 DE SEGURANÇA

1.6.1 A fornecedora da solução deverá obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pela JUSTIÇA ELEITORAL, em especial:

1.6.1.1 O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do TRE/RN a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.

1.6.1.2 Da gestão de ativos.

1.6.1.3 Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da JUSTIÇA ELEITORAL ou de terceiros de que tomar conhecimento em razão da execução do objeto desta contratação devendo orientar seus funcionários nesse sentido.

1.6.1.4 Submeter seus recursos técnicos aos regulamentos de segurança e disciplina instituídos pela JUSTIÇA ELEITORAL, durante o tempo de permanência nas suas dependências, observando a Portaria 226/2018-GP-TRE/RN, que dispõe sobre as medidas de controle de acesso, circulação e permanência de pessoas nos prédios do Edifício-Sede do Tribunal Regional Eleitoral do Rio Grande do Norte, do Centro de Operações da Justiça Eleitoral (COJE), Fórum Eleitoral de Natal e, no que couber, aos prédios das Zonas Eleitorais do Interior do Estado.

1.7 SOCIAIS, AMBIENTAIS E CULTURAIS

1.7.1 É de responsabilidade da empresa fornecedora da solução a disposição final responsável e ambientalmente adequada das embalagens e materiais que porventura venham a ser utilizados em observância à Logística Reversa disposta no art. 33 da Lei Nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos.

1.7.2 O Tribunal Regional Eleitoral do Rio Grande do Norte reserva-se o direito de assumir a responsabilidade a que se refere o item anterior, podendo dar outra destinação às embalagens e materiais após o uso, caso julgue mais conveniente para a Administração.

1.7.3 Qualquer material que venha a ser utilizado na embalagem dos produtos ofertados e/ou utilizados na execução dos serviços deverão ter sua reciclabilidade efetiva no Brasil.

1.7.4 A documentação e os manuais da solução deverão, preferencialmente, ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em Inglês.

1.7.4.1 Todos os contatos para gerenciamento de chamados e suporte técnico deverão ser realizados em Português (Brasil).

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

1.7.6 Os *softwares* aplicativos e suas interfaces devem ter a possibilidade de escolha de idioma pelo usuário.

1.7.6.1 Será admitido o idioma Inglês somente quando não existir uma versão no idioma Português do Brasil.

1.7.7 Os profissionais da fornecedora da solução deverão trajar-se de maneira respeitável e usar linguagem respeitosa e formal no trato com os servidores do órgão, Gestão Contratual e os dirigentes do TRE/RN.

1.8 DE ARQUITETURA TECNOLÓGICA

1.8.1 Caso a solução seja um *Appliance* Físico:

1.8.1.1 Os *appliances* físicos devem ser novos e de primeiro uso.

1.8.1.2 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.

1.8.1.3 Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento.

1.8.1.3.1 Não devem ser remanufaturados, recondicionados ou possuir reparos de qualquer espécie.

1.8.1.4 Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo *end-of-sale*, *end-ofsupport* ou *end-of-life* do fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante.

1.8.1.5 O equipamento deve se instalar em *rack* com largura padrão de 19 (dezenove) polegadas, padrão

EIA-310, ocupando no máximo 2Us do referido *rack*.

1.8.1.6 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*.

1.8.1.7 Deve ser fornecido com todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento.

1.8.1.8 Dispor de fonte de alimentação redundante com tensão de entrada de *110 V* a *220 V* AC automática e frequência de 60 Hz.

1.8.1.9 Possuir sistema operacional customizado especificamente para funções de *Web Application Firewall*, não podendo ser entregue *appliance* do tipo *NGFW.*

1.8.1.10 Possuir, no mínimo, 06 interfaces, sendo 02 de 10GE com conectores padrão SFP+ (SR) e 04 portas SFP e *transceivers* (SR ou UTP).

1.8.1.10.1 Serão aceitas interfaces de maior capacidade, desde que possibilitem ser transformados em 10 GE (incluindo os cabos "*breakout*" de no mínimo 3 metros).

1.8.1.11 Possuir 01(uma) interfaces 1GE, incluso interfaces de gerência com conectores padrão RJ45.

1.8.1.12 Todas as interfaces fornecidas devem estar licenciadas e habilitadas para uso imediato.

1.8.1.13 Possuir no mínimo de 8.000 Mbps de *throughput* em camada 7.

1.8.1.14 Possuir capacidade de 4.000 transações por segundo (*TPS*) em *TLS* padrão *RSA* (chaves de 2.048 bit).

1.8.1.15 Possuir no mínimo compressão em *hardware* de 5.000 Mbps em (tráfego *HTTP/HTTPS*).

1.8.1.16 Recursos de agregação de portas baseado no protocolo *LACP*, segundo o padrão *IEEE* 802.3ad.

1.8.1.17 Memória RAM mínima de 16 GB.

1.8.1.18 Disco rígido com capacidade de armazenamento interno e retenção de *logs* para análise ser de no mínimo 1TB.

1.8.1.19 Deve vir acompanhado de todas as licenças de *software* ou *hardware* necessárias para atendimento das funcionalidades exigidas neste caderno de especificações técnicas.

1.8.1.20 Todas as funcionalidades devem continuar ativas, mesmo após o término do termo de garantia e suporte técnico.

1.8.1.21 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.

1.8.1.22 Suportar e garantir a instalação em ambiente de alta disponibilidade.

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

1.8.1.24 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.

1.8.1.25 Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá

"*downtime*" e queda de sessões em caso de falha de uma das unidades.

1.8.1.26 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.

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

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

1.8.1.29 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.

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

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

1.8.1.32 Analisar e proteger tráfego *HTTP/1.0, HTTP/1.1, HTTP/2.0 e HTTP/3*;

1.8.1.33 Possuir suporte a *IPv6*;

1.8.1.34 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.

1.8.1.35 Deve suportar, no mínimo, 1000 *VLANs* simultaneamente.

1.8.1.36 Implementar o *SNTP (Simple Network Time Protocol)* ou *NTP (Network Time Protocol).*

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

1.8.1.38 Assinar *cookies* digitalmente e editar endereços de *URL ("URL Rewriting").*

1.8.1.39 O equipamento deverá permitir a sincronização das configurações:

1.8.1.39.1 De forma automática;

1.8.1.39.2 Manualmente, forçando a sincronização apenas no momento desejado;

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

1.8.1.40.1 Compartilhar a rede de *heartbeat* com a rede de dados;

1.8.1.40.2 Utilizar uma rede exclusiva para o *heartbeat*.

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

1.8.1.42 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.

1.8.1.43 Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos *scripts*.

1.8.1.44 Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores: *GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version*.

1.8.1.45 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*.

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

1.8.1.47 Permitir acesso *in-band* via *SSH*.

1.8.1.48 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.

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

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

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

1.8.1.50 Manter internamente múltiplos arquivos de configurações do sistema.

1.8.1.51 Utilizar *SCP* ou *HTTPS* como mecanismo de transferência de arquivos de configuração e sistema operacional.

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

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

1.8.1.54 Possuir Interface Gráfica via *Web*.

1.8.1.55 Possuir auto-complementação de comandos na *CLI*.

1.8.1.56 Possuir ajuda contextual.

1.8.1.57 A Solução deve ter a capacidade de permitir a criação de *MIBs* customizadas.

1.8.1.58 A Solução deve ter suporte a *sFlow*.

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

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

1.8.1.61 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.

1.8.1.62 A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o *boot.*

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

1.8.1.64 Suportar a *rollback* de configuração e imagem.

1.8.1.65 Possuir e fornecer geração de mensagens de *syslog* para eventos relevantes ao sistema.

1.8.1.66 Possuir configuração de múltiplos *syslog servers* para os quais o equipamento enviará as mensagens de *syslog.*

1.8.1.67 Possuir armazenamento de mensagens de *syslog* em dispositivo interno ao equipamento.

1.8.1.68 A interface Gráfica deverá permitir a reinicialização do equipamento.

1.8.1.69 Reinicialização do equipamento por comando na *CLI*.

1.8.1.70 Possuir recurso de gerência via *SNMP* e implementar *SNMPv1, SNMPv2c e SNMPV3.*

1.8.1.71 Possuir *traps SNMP.*

1.8.1.72 Possuir suporte a monitoração utilizando *RMON* através de pelo menos 04 (quatro) grupos: *statistics, history, alarms* e *events.*

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

1.8.1.74 Implementar *Debugging*: *CLI* via console e *SSH*.

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

1.8.1.76 Permitir a criação de políticas diferenciadas por aplicação.

1.8.1.77 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.

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

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

1.8.1.80 Permitir as seguintes opções de implementação:

1.8.1.80.1 Monitoramento (sem bloqueio).

1.8.1.80.2 *Proxy* (reverso e transparente).

1.8.1.81 Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento.

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

1.8.1.83 Em modo “monitoramento” (sem bloqueio), realizar análise e avaliação do tráfego, gerar relatórios com os dados analisados e simular bloqueios para efeito de avaliação.

1.8.1.84 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.

1.8.1.85 Bloquear ataques aos servidores de aplicação, por meio dos recursos de identificação, isolamento e bloqueio de ataques sofisticados sem impactar nas transações das aplicações.

1.8.1.86 Possuir *firewall XML* integrado com suporte a filtro e validação de funções *XML* específicas da aplicação.

1.8.1.87 A solução deve suportar e fazer a proteção do tráfego de protocolo *WebSocket*.

1.8.1.88 A solução deve suportar o uso de páginas de login *AJAX/JSON* tanto com configuração manual como descoberta automática.

1.8.1.89 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*.

1.8.1.90 Quando detectada uma tentativa de ataque bloquear de imediato o tráfego ou a sessão.

1.8.1.91 Bloqueio com intermediação e interrupção da conexão.

1.8.1.92 Criação de políticas automáticas que bloqueiam o endereço *IP* que realizar violações.

1.8.1.93 Utilização de página *HTML* informativa e personalizável como *HTTP Response* aos bloqueios.

1.8.1.94 Configuração de políticas de bloqueio baseadas em requisição *HTTP*, endereço *IP* e usuário de aplicação.

1.8.1.95 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.

1.8.1.96 Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:

1.8.1.96.1 Endereços IP que originaram os ataques;

1.8.1.96.2 Horário do ataque;

1.8.1.96.3 Nome do ataque;

1.8.1.96.4 Qual campo foi atacado;

1.8.1.96.5 Quantas vezes esse ataque foi realizado.

1.8.1.97 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.*

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

1.8.1.99 Identificar ataques baseados em:

1.8.1.99.1 Assinaturas, com atualização diária da base pelo fabricante.

1.8.1.99.2 Regras.

1.8.1.99.3 Perfis de utilização.

1.8.1.100 Deve possuir tecnologia para mitigação de *DDoS* em camada 7 baseado em análise comportamental, usando o aprendizado.

1.8.1.101 Não deve haver a necessidade de intervenção de usuário para configurar *thresholds DoS* pois esses valores devem ser autoajustáveis e adaptativos de acordo com mudanças.

1.8.1.102 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.

1.8.1.103 Detectar ataques de força bruta por meio dos seguintes métodos:

1.8.1.103.1 Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;

1.8.1.103.2 Quantidade de transações por segundo (*TPS*), monitorando a quantidade de transações por segundo por endereço IP.

1.8.1.104 Detectar ataques do tipo força bruta em que:

1.8.1.104.1 O atacante solicita repetidamente o mesmo recurso.

1.8.1.104.2 O atacante realiza repetidas tentativas não autorizadas de acesso.

1.8.1.104.3 São utilizados ataques automatizados de login.

1.8.1.105 Detectar ataques do tipo força bruta que explorem:

1.8.1.105.1 Controles de acesso da aplicação (Erro 401 – *Unauthorized*);

1.8.1.105.2 Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação.

1.8.1.105.3 Aplicações WEB que não retornam o Erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação.

1.8.1.105.4 Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um range de Ips).

1.8.1.105.5 Clientes automatizados (robôs, requisições muito rápidas).

1.8.1.105.6 Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes.

1.8.1.105.7 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.

1.8.1.105.8 Possibilitar atualização de novas assinaturas para ataques conhecidos.

1.8.1.106 Apresentar proteção contra-ataques, como:

1.8.1.106.1 Brute Force Login.

1.8.1.106.2 Buffer Overflow.

1.8.1.106.3 Cookie Injection.

1.8.1.106.4 Cookie Poisoning.

1.8.1.106.5 Cross Site Request Forgery (CSRF).

1.8.1.106.6 Cross Site Scripting (XSS).

1.8.1.106.7 Server Side Request Forgery (SSRF).

1.8.1.106.8 Directory Traversal.

1.8.1.106.9 Forceful Browsing.

1.8.1.106.10 HTTP Denial of Service.

1.8.1.106.11 HTTP hidden field manipulation.

1.8.1.106.12 HTTP request smuggling.

1.8.1.106.13 HTTP Response Splitting.

1.8.1.106.14 Malicious Robots.

1.8.1.106.15 Parameter Tampering.

1.8.1.106.16 Remote File Inclusion Attacks.

1.8.1.106.17 Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI).

1.8.1.106.18 Session Hijacking.

1.8.1.106.19 SQL Injection.

1.8.1.106.20 Web Scraping.

1.8.1.106.21 Web server software and operating system attacks.

1.8.1.106.22 Web Services (XML) attacks.

1.8.1.107 Permitir configurar granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de *cookies*;

1.8.1.108 Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:

1.8.1.108.1 Assinatura de ataque.

1.8.1.108.2 Código de *response.*

1.8.1.108.3 Conteúdo da *cookie.*

1.8.1.108.4 Conteúdo do cabeçalho.

1.8.1.108.5 Conteúdo do *payload.*

1.8.1.108.6 Hostname.

1.8.1.108.7 IP de origem.

1.8.1.108.8 Método HTTP.

1.8.1.108.9 Número de ocorrências em determinado intervalo de tempo.

1.8.1.108.10 Parâmetro.

1.8.1.108.11 *User-agent* (navegador).

1.8.1.109 Permitir a criação de assinaturas de ataques.

1.8.1.110 Reconhecer assinaturas seletivas, e filtros de ataque que devem proteger contra:

1.8.1.110.1 Ataques de negação de serviços automatizados.

1.8.1.110.2 *Worms* e vulnerabilidades conhecidas.

1.8.1.110.3 *Requests* em objetos restritos.

1.8.1.111 Deve proteger contra ataques *SSRF (Server Side RequestForgery*).

1.8.1.112 A solução oferecida deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos.

1.8.1.112.1 Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra.

1.8.1.113 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.

1.8.1.114 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.

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

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

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

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

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

1.8.1.120 Possuir método de mitigação de *DoS L7* baseado em:

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

1.8.1.120.2 CAPTCHA para suspeitos que ultrapassarem os *thresholds.*

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

1.8.1.121 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.*

1.8.1.122 Aprender o comportamento da aplicação:

1.8.1.122.1 Campos, valores, *cookies e URLs*.

1.8.1.123 Políticas sugeridas somente devem ser aplicadas após um período configurável.

1.8.1.124 Inspecionar 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*.

1.8.1.125 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*.

1.8.1.126 Proteger contra mensagens *XML* e *SOAP* malformadas.

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

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

1.8.1.129 Deverá permitir o bloqueio de robôs (*bots*) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais.

1.8.1.129.1 Robôs conhecidos do mercado, como *Google*, *Yahoo* e *Microsoft Bing* deverão ser liberados por padrão.

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

1.8.1.131 Deverá implementar proteção ao *JSON (JavaScript Object Notation)*.

1.8.1.132 Implementar a segurança de *web services*, através dos seguintes métodos:

1.8.1.132.1 Criptografar/Decriptografar partes das mensagens *SOAP.*

1.8.1.132.2 Assinar digitalmente partes das mensagens *SOAP.*

1.8.1.132.3 Verificação de partes das mensagens *SOAP*.

1.8.1.133 Deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas.

1.8.1.133.1 Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável.

1.8.1.134 Deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação.

1.8.1.134.1 Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação.

1.8.1.135 Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no *browser* do usuário.

1.8.1.135.1 Deve proteger esses dados criptografados de *malwares e keyloggers.*

1.8.1.136 Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos.

1.8.1.136.1 Esse nome de parâmetro deve ser mudado constantemente pela ferramenta para dificultar ataques direcionados.

1.8.1.137 Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação.

1.8.1.137.1 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.

1.8.1.138 A solução deverá se integrar a soluções de análise (*Scanner*) de vulnerabilidade do site.

1.8.1.138.1 O resultado desta análise deve ser utilizado para configurar as políticas do equipamento.

1.8.1.139 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*.

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

1.8.1.140.1 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.

1.8.1.141 Deverá permitir o agendamento de relatórios a serem entregues por e-mail.

1.8.1.142 Emitir os seguintes relatórios gráficos dos alterar por:

1.8.1.142.1 Política de segurança.

1.8.1.142.2 Tipos de ataques.

1.8.1.143 Violações.

1.8.1.144 URL que foram atacadas.

1.8.1.145 Endereços IP de origem.

1.8.1.146 Localização geográfica dos endereços IPs de origem.

1.8.1.147 Severidade.

1.8.1.148 Código de resposta.

1.8.1.149 Métodos.

1.8.1.150 Protocolos.

1.8.1.151 Sessão.

1.8.1.152 Permitir a seleção de período para emissão dos relatórios.

1.8.1.153 Permitir a geração das seguintes informações, por período:

1.8.1.153.1 Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário.

1.8.1.153.2 Informações estatísticas de quantidade de conexões completadas e bloqueadas.

1.8.1.153.3 Informações estatísticas de fluxo de tráfego.

1.8.1.153.4 Informações estatísticas de quantidade de sessões ou conexões.

1.8.1.154 Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: *HTTP e HTTPS*.

1.8.1.155 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.

1.8.1.156 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.

1.8.1.157 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.

1.8.1.158 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.

1.8.1.159 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:

1.8.1.159.1 *SSL session cache Timeout*;

1.8.1.159.2 *Session Ticket*;

1.8.1.159.3 *OCSP (Online Certificate Status Protocol) Stapling*;

1.8.1.159.4 *Dynamic Record Sizing*;

1.8.1.159.5 *ALPN (Application Layer Protocol Negotiation)*;

1.8.1.159.6 *Perfect Forward Secrecy*.

1.8.1.160 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:

1.8.1.160.1 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;

1.8.1.160.2 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*;

1.8.1.160.3 Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;

1.8.1.160.4 Ao realizar inspeção, proteção, *OffLoad* e aceleração de tráfego criptografado através de *SSL/TLS*;

1.8.1.160.5 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*.

1.8.1.161 Deve possibilitar a customização da interface gráfica da página de login e mensagens de apresentação ao usuário de acordo com o grupo que pertença.

1.8.1.162 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:

1.8.1.162.1 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.

1.8.1.162.2 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.

1.8.1.162.3 Modo “*Network*”, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna.

1.8.1.162.4 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.

1.8.1.163 Deverá ser capaz de autenticar usuários em bases de dados *LDAP, Radius, Tacacs+, Kerberos e RSA SecurID*.

1.8.1.164 Deve suportar autenticação de múltiplos fatores utilizando *tokens* de *Hardware* ou *one-time passcode (OTP).*

1.8.1.165 Deve possuir capacidade para realizar *proxy* reverso com a finalidade de omitir a URI real, promovendo assim o acesso seguro as aplicações web internas.

1.8.1.166 Deverá prover acesso remoto através de *VPN SSL* para Microsoft Windows, Linux, dispositivos baseados em Android e iOS e *MAC OSX*.

1.8.1.167 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.

1.8.1.168 Melhora da disponibilidade das aplicações através do balanceamento da entrada de tráfego deve possuir, ao menos, as seguintes características:

1.8.1.168.1 *DNS* autoritativo.

1.8.1.168.2 *DNS* secundário.

1.8.1.168.3 *DNS* resolver.

1.8.1.168.4 *DNS* cache.

1.8.1.168.5 Balanceamento de *DNS servers.*

1.8.1.168.6 *DNSSec*.

1.8.1.169 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*.

1.8.1.170 A solução deve realizar o *offload* dos servidores de *DNS*, funcionando como o *DNS* secundário.

1.8.1.171 A solução deve suportar pelo menos os seguintes tipos de requisição *DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT*.

1.8.1.172 Deve ser capaz de gerar estatísticas sobre consultas de *DNS* por: Aplicação, nome da query, tipo da *query*, endereço IP do cliente.

1.8.1.173 Deve ser possível configurar a solução de modo *inline* a estrutura de *DNS* existente e transparente sem requerer grandes mudanças na infraestrutura.

1.8.1.174 Deve prover as respostas a *queries DNS* da própria *RAM CACHE*.

1.8.1.175 A solução deve ser capaz de realizar *IP Anycast*.

1.8.1.176 A solução deve ser capaz de realizar *DNSSec*, independente da estrutura dos servidores *DNS* em uso.

1.8.1.177 A solução de alta disponibilidade não deve depender de *BGP* ou outro protocolo de roteamento.

1.8.1.178 Suportar pelo menos os seguintes algoritmos de balanceamento:

1.8.1.178.1 Round Robin.

1.8.1.178.2 Global Availability.

1.8.1.178.3 Ratio.

1.8.1.178.4 LDNS Persist.

1.8.1.178.5 Geografia.

1.8.1.178.6 Disponibilidade da Aplicação.

1.8.1.178.7 Capacidade do *Virtual Server.*

1.8.1.178.8 Least Connections.

1.8.1.178.9 Pacotes por segundo.

1.8.1.178.10 Round trip time.

1.8.1.178.11 Hops.

1.8.1.178.12 Packet Completion Rate.

1.8.1.178.13 *QoS* definido pelo usuário.

1.8.1.178.14 *Kilobytes per Second*.

1.8.1.179 A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com *IPv4 (requests AAAA ou A6)*.

1.8.1.180 A solução deve suportar *edns-client-subnet (ECS)* para tanto responder requisições de clientes ou encaminhar requisições de clientes (*screening*).

1.8.1.181 Baseado no *ECS DNS* deve ser possível preservar o endereço IP da *subnet* do cliente ao invés do *LDNS* para tomar decisões.

1.8.1.182 A solução deve funcionar pelo menos das seguintes formas:

1.8.1.182.1 Usar o *ECS* para tomar decisões baseado em topologia (*Subnets*).

1.8.1.182.2 Injetar o *ECS (proxy requests)* para outros servidores DNS.

1.8.1.183 A solução deve fazer persistência baseado no endereço IP do cliente (*ECS*), significando que se o cliente mudar de *LDNS* resolver (suporte *ECS*).

1.8.1.184 Possuir recursos para executar compressão de conteúdo *HTTP*, para reduzir a quantidade de informações enviadas ao cliente.

1.8.1.185 Definir qual tipo de compressão será habilitada (*gzip1 a gzip9, deflate*).

1.8.1.186 Possuir capacidade para definir compressão especificamente para certos tipos de objetos.

1.8.1.187 Permitir o balanceamento de aplicações em um pool de servidores, independentemente do hardware, sistema operacional e tipo de aplicação.

1.8.1.188 Suportar os seguintes métodos de balanceamento:

1.8.1.188.1 Round Robin.

1.8.1.188.2 Least Connection.

1.8.1.188.3 Por peso.

1.8.1.188.4 Servidor ou equipamento com resposta mais rápida baseado no tráfego real.

1.8.1.188.5 *Weighted Percentage* dinâmico (baseado no número de conexões).

1.8.1.188.6 Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via *SNMP* ou *WMI*.

1.8.1.189 A solução deve permitir aplicar criptografia de *cookies* para a proteção dos *cookies* utilizados pela aplicação web.

1.8.1.190 Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

1.8.1.190.1 Por *cookie.*

1.8.1.190.2 Endereço de origem.

1.8.1.190.3 Sessão *SSL.*

1.8.1.190.4 Análise da URL acessada.

1.8.1.190.5 Através de qualquer parâmetro do cabeçalho *HTTP.*

1.8.1.190.6 Através da análise do *MS Terminal Services Session (MSRDP*).

1.8.1.190.7 Através da análise do *SIP Call ID ou Source IP.*

1.8.1.191 Através da análise de qualquer informação da porção de dados (camada 7).

1.8.1.192 O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:

1.8.1.192.1 ICMP, TCP, HTTP, HTTPs.

1.8.1.192.2 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.*

1.8.1.193 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor.

1.8.1.194 Realizar *Network Address Translation (NAT)*.

1.8.1.195 Realizar proteção contra *syn flood*.

1.8.1.196 Realizar as proteções de cabeçalho: *X-Frame-Options, X-XSS-Protection, X-Content- Type- Options*.

1.8.1.197 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 atividades maliciosas ou ataques de rede.

1.8.1.198 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.

1.8.1.198.1 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.

1.8.1.198.2 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.

1.8.1.199 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.

1.8.1.200 A solução deve utilizar *Cache Array Routing Protocol (CARP)* no algoritmo de *HASH*.

1.8.1.201 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real.

1.8.1.202 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual.

1.8.1.203 Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores.

1.8.1.204 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico.

1.8.1.205 Realizar *Network Address Translation (NAT)*.

1.8.1.206 Realizar Proteção contra *Denial of Service (DoS)*.

1.8.1.207 Realizar Proteção contra *Syn flood*.

1.8.1.208 Realizar Limpeza de cabeçalho *HTTP*.

1.8.1.209 Deve possuir suporte a *Link Layer Discovery Protocol (LLDP)*.

1.8.1.210 Deve ser possível enviar, pelo menos, as seguintes informações via *LLDP*:

1.8.1.210.1 *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*.

1.8.1.211 Suporte a otimização do protocolo *TCP* para ajustes a parâmetros das conexões clientes e servidor.

1.8.1.212 Deve ser capaz de realizar *DHCP relay*.

1.8.1.213 Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:

1.8.1.213.1 Tempo de resposta da aplicação.

1.8.1.213.2 Latência.

1.8.1.213.3 Conexões para conjunto de servidores, servidores individuais.

1.8.1.213.4 Por *URL.*

1.8.1.213.5 A solução deve ter suporte a *TLS* 1.3.

1.8.2 Caso a solução seja um Appliance Virtual:

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

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

1.8.2.3 A solução deve ser licenciada para uso perpétuo.

1.8.2.3.1 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.

1.8.2.4 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*).

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

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

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

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

1.8.2.9 Suportar e garantir a instalação em ambiente de alta disponibilidade.

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

1.8.2.11 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.

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

1.8.2.13 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.

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

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

1.8.2.16 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.

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

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

1.8.2.19 Analisar e proteger tráfego *HTTP/1.0, HTTP/1.1, HTTP/2.0 e HTTP/3.*

1.8.2.20 Possuir suporte a *IPv6*.

1.8.2.21 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.

1.8.2.22 Deve suportar, no mínimo, 1000 *VLANs* simultaneamente.

1.8.2.23 Implementar o *SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);*

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

1.8.2.25 Assinar *cookies* digitalmente e editar endereços de *URL ("URL Rewriting").*

1.8.2.26 O equipamento deverá permitir a sincronização das configurações:

1.8.2.26.1 De forma automática.

1.8.2.26.2 Manualmente, forçando a sincronização apenas no momento desejado;

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

1.8.2.27.1.1 Compartilhar a rede de *heartbeat* com a rede de dados;

1.8.2.27.1.2 Utilizar uma rede exclusiva para o *heartbeat*.

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

1.8.2.29 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.

1.8.2.30 Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos *scripts*.

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

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

1.8.2.32 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.*

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

1.8.2.34 Permitir acesso *in-band* via *SSH*.

1.8.2.35 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.

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

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

1.8.2.36.2 Permitir a replicação de configurações e a aplicação de atualização de softwares para os

elementos dos nós do *cluster.*

1.8.2.37 Manter internamente múltiplos arquivos de configurações do sistema.

1.8.2.38 Utilizar *SCP* ou *HTTPS* como mecanismo de transferência de arquivos de configuração e Sistema Operacional.

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

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

1.8.2.41 Possuir Interface Gráfica via *Web*.

1.8.2.42 Possuir auto-complementação de comandos na *CLI*.

1.8.2.43 Possuir ajuda contextual.

1.8.2.44 A Solução deve ter a capacidade de permitir a criação de *MIBs* customizadas.

1.8.2.45 A Solução deve ter suporte a *sFlow*.

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

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

1.8.2.48 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.

1.8.2.49 A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o *boot.*

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

1.8.2.51 Suportar a *rollback* de configuração e imagem.

1.8.2.52 Possuir e fornecer geração de mensagens de *syslog* para eventos relevantes ao sistema.

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

1.8.2.54 Possuir armazenamento de mensagens de *syslog* em dispositivo interno ao equipamento.

1.8.2.55 A interface Gráfica deverá permitir a reinicialização do equipamento.

1.8.2.56 Reinicialização do equipamento por comando na *CLI*.

1.8.2.57 Possuir recurso de gerência via *SNMP* e implementar *SNMPv1, SNMPv2c e SNMPV3.*

1.8.2.58 Possuir *traps SNMP.*

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

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

1.8.2.61 Implementar *Debugging*: CLI via console e *SSH.*

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

1.8.2.63 Permitir a criação de políticas diferenciadas por aplicação.

1.8.2.64 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.

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

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

1.8.2.67 Permitir as seguintes opções de implementação:

1.8.2.67.1 Monitoramento (sem bloqueio).

1.8.2.67.2 *Proxy* (reverso e transparente).

1.8.2.68 Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento.

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

1.8.2.70 Em modo "monitoramento" (sem bloqueio), realizar análise e avaliação do tráfego, gerar relatórios com os dados analisados e simular bloqueios para efeito de avaliação.

1.8.2.71 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.

1.8.2.72 Bloquear ataques aos servidores de aplicação, por meio dos seguintes recursos:

1.8.2.72.1 Identificação, isolamento e bloqueio de ataques sofisticados sem impactar nas transações das aplicações.

1.8.2.73 Possuir *firewall* XML integrado com suporte a filtro e validação de funções XML específicas da aplicação.

1.8.2.74 A solução deve suportar e fazer a proteção do tráfego de protocolo *WebSocket.*

1.8.2.75 A solução deve suportar o uso de páginas de *login AJAX/JSON* tanto com configuração manual como descoberta automática.

1.8.2.76 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.*

1.8.2.77 Quando detectada uma tentativa de ataque bloquear de imediato o tráfego ou a sessão.

1.8.2.78 Bloqueio com intermediação e interrupção da conexão.

1.8.2.79 Criação de políticas automáticas que bloqueiam o endereço *IP* que realizar violações.

1.8.2.80 Utilização de página *HTML* informativa e personalizável como *HTTP* Response aos bloqueios,

1.8.2.81 Configuração de políticas de bloqueio baseadas em requisição *HTTP*, endereço *IP* e usuário de aplicação.

1.8.2.82 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.

1.8.2.83 Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:

1.8.2.83.1 Endereços IP que originaram os ataques.

1.8.2.83.2 Horário do ataque.

1.8.2.83.3 Nome do ataque.

1.8.2.83.4 Qual campo foi atacado.

1.8.2.83.5 Quantas vezes esse ataque foi realizado.

1.8.2.84 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.*

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

1.8.2.86 Identificar ataques baseados em:

1.8.2.86.1 Assinaturas, com atualização diária da base pelo fabricante.

1.8.2.86.2 Regras.

1.8.2.86.3 Perfis de utilização.

1.8.2.87 Deve possuir tecnologia para mitigação de *DDoS* em camada 7 baseado em análise comportamental, usando o aprendizado.

1.8.2.88 Não deve haver a necessidade de intervenção de usuário para configurar *thresholds DoS* pois esses valores devem ser autoajustáveis e adaptativos de acordo com mudanças.

1.8.2.89 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.

1.8.2.90 Detectar ataques de força bruta por meio dos seguintes métodos:

1.8.2.90.1 Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;

1.8.2.90.2 Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP.

1.8.2.91 Detectar ataques do tipo força bruta em que:

1.8.2.91.1 O atacante solicita repetidamente o mesmo recurso.

1.8.2.91.2 O atacante realiza repetidas tentativas não autorizadas de acesso.

1.8.2.91.3 São utilizados ataques automatizados de login.

1.8.2.92 Detectar ataques do tipo força bruta que explorem:

1.8.2.92.1 Controles de acesso da aplicação (Erro 401 – *Unauthorized).*

1.8.2.92.2 Solicitações repetidas ao mesmo recurso, em qualquer parte/*URL* da aplicação.

1.8.2.92.3 Aplicações *WEB* que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação.

1.8.2.92.4 Gerenciamento de sessão (muitas sessões de um único endereço *IP* ou a um *range de Ips*).

1.8.2.92.5 Clientes automatizados (robôs, requisições muito rápidas).

1.8.2.92.6 Permitir a criação de políticas diferenciadas por aplicação e por *URL*, onde cada aplicação e *URL* poderão ter políticas totalmente diferentes.

1.8.2.92.7 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.

1.8.2.92.8 Possibilitar atualização de novas assinaturas para ataques conhecidos.

1.8.2.93 Apresentar proteção contra-ataques, como:

1.8.2.93.1 Brute Force Login.

1.8.2.93.2 Buffer Overflow.

1.8.2.93.3 Cookie Injection.

1.8.2.93.4 Cookie Poisoning.

1.8.2.93.5 Cross Site Request Forgery (CSRF).

1.8.2.93.6 Cross Site Scripting (XSS).

1.8.2.93.7 Server Side Request Forgery (SSRF).

1.8.2.93.8 Directory Traversal.

1.8.2.93.9 Forceful Browsing.

1.8.2.93.10 HTTP Denial of Service.

1.8.2.93.11 HTTP hidden field manipulation.

1.8.2.93.12 HTTP request smuggling.

1.8.2.93.13 HTTP Response Splitting.

1.8.2.93.14 Malicious Robots.

1.8.2.93.15 Parameter Tampering.

1.8.2.93.16 Remote File Inclusion Attacks.

1.8.2.93.17 Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI).

1.8.2.93.18 Session Hijacking.

1.8.2.93.19 SQL Injection.

1.8.2.93.20 Web Scraping.

1.8.2.93.21 Web server software and operating system attacks.

1.8.2.93.22 Web Services (XML) attacks.

1.8.2.94 Permitir configurar, granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de *cookies.*

1.8.2.95 Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:

1.8.2.95.1 Assinatura de ataque.

1.8.2.95.2 Código de response.

1.8.2.95.3 Conteúdo da *cookie.*

1.8.2.95.4 Conteúdo do cabeçalho.

1.8.2.95.5 Conteúdo do *payload.*

1.8.2.95.6 Hostname.

1.8.2.95.7 IP de origem.

1.8.2.95.8 Método *HTTP.*

1.8.2.95.9 Número de ocorrências em determinado intervalo de tempo.

1.8.2.95.10 Parâmetro.

1.8.2.95.11 *User-agent* (navegador).

1.8.2.96 Permitir a criação de assinaturas de ataques.

1.8.2.97 Reconhecer assinaturas seletivas, e filtros de ataque que devem proteger contra:

1.8.2.97.1 Ataques de negação de serviços automatizados.

1.8.2.97.2 *Worms* e vulnerabilidades conhecidas.

1.8.2.97.3 *Requests* em objetos restritos.

1.8.2.98 Deve proteger contra ataques *SSRF (Server Side RequestForgery).*

1.8.2.99 A solução oferecida deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos.

1.8.2.99.1 Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra.

1.8.2.100 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.

1.8.2.101 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.

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

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

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

1.8.2.105 Ao detectar uma condição de *DDoS*, assinaturas dinâmicas devem ser automaticamente criadas

e implementadas em tempo real para proteção da aplicação.

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

1.8.2.107 Possuir método de mitigação de *DoS* L7 baseado em:

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

1.8.2.107.2 CAPTCHA para suspeitos que ultrapassarem os *thresholds.*

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

1.8.2.108 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.*

1.8.2.109 Aprender o comportamento da aplicação:

1.8.2.109.1 Campos, valores, *cookies e URLs.*

1.8.2.110 Políticas sugeridas somente devem ser aplicadas após um período configurável.

1.8.2.111 Inspecionar 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.*

1.8.2.112 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.*

1.8.2.113 Proteger contra mensagens *XML* e *SOAP* malformadas.

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

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

1.8.2.116 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.

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

1.8.2.118 Deverá implementar proteção ao *JSON (JavaScript Object Notation).*

1.8.2.119 Implementar a segurança de *web services*, através dos seguintes métodos:

1.8.2.119.1 Criptografar/Decriptografar partes das mensagens *SOAP.*

1.8.2.119.2 Assinar digitalmente partes das mensagens *SOAP.*

1.8.2.119.3 Verificação de partes das mensagens *SOAP.*

1.8.2.120 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.

1.8.2.121 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.

1.8.2.122 Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no *browser* do usuário.

1.8.2.122.1 Deve proteger esses dados criptografados de *malwares* e *keyloggers*.

1.8.2.123 Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos.

1.8.2.123.1 Esse nome de parâmetro deve ser mudado constantemente pela ferramenta para dificultar ataques direcionados.

1.8.2.124 Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação.

1.8.2.124.1 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.

1.8.2.125 A solução deverá se integrar a soluções de análise (*Scanner*) de vulnerabilidade do site.

1.8.2.125.1 O resultado desta análise deve ser utilizado para configurar as políticas do equipamento.

1.8.2.126 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*.

1.8.2.127 A solução deve fornecer relatórios consolidados de ataques com, pelo menos, os seguintes dados:

1.8.2.127.1 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.

1.8.2.128 Deverá permitir o agendamento de relatórios a serem entregues por *e-mail.*

1.8.2.129 Emitir os seguintes relatórios gráficos por:

1.8.2.129.1 Política de segurança.

1.8.2.129.2 Tipos de ataques.

1.8.2.129.3 Violações.

1.8.2.129.4 URL que foram atacadas.

1.8.2.129.5 Endereços IP de origem.

1.8.2.129.6 Localização geográfica dos endereços IPs de origem.

1.8.2.129.7 Severidade.

1.8.2.129.8 Código de resposta.

1.8.2.129.9 Métodos.

1.8.2.129.10 Protocolos.

1.8.2.129.11 Sessão.

1.8.2.130 Permitir a seleção de período para emissão dos relatórios.

1.8.2.131 Permitir a geração das seguintes informações, por período:

1.8.2.131.1 Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação

e horário.

1.8.2.131.2 Informações estatísticas de quantidade de conexões completadas e bloqueadas.

1.8.2.131.3 Informações estatísticas de fluxo de tráfego.

1.8.2.131.4 Informações estatísticas de quantidade de sessões ou conexões.

1.8.2.132 Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: *HTTP e HTTPS.*

1.8.2.133 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.

1.8.2.134 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.

1.8.2.135 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.

1.8.2.136 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.

1.8.2.137 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:

1.8.2.137.1 SSL session cache Timeout.

1.8.2.137.2 Session Ticket.

1.8.2.137.3 OCSP (Online Certificate Status Protocol) Stapling.

1.8.2.137.4 Dynamic Record Sizing.

1.8.2.137.5 ALPN (Application Layer Protocol Negotiation).

1.8.2.137.6 Perfect Forward Secrecy.

1.8.2.138 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:

1.8.2.138.1 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;*

1.8.2.138.2 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.*

1.8.2.138.3 Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;

1.8.2.138.4 Ao realizar inspeção, proteção, *OffLoad* e aceleração de tráfego criptografado através de *SSL/TLS.*

1.8.2.138.5 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.

1.8.2.139 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.

1.8.2.140 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:

1.8.2.140.1 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.

1.8.2.140.2 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.

1.8.2.140.3 Modo "*Network*", onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna.

1.8.2.140.4 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.

1.8.2.141 Deverá ser capaz de autenticar usuários em bases de dados *LDAP, Radius, Tacacs+, Kerberos e RSA SecurID.*

1.8.2.142 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.

1.8.2.143 Deverá prover acesso remoto através de *VPN SSL* para *Microsoft Windows, Linux,* dispositivos/baseados em Android e *iOS e MAC OSX.*

1.8.2.144 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.

1.8.2.145 Melhora da disponibilidade das aplicações através do balanceamento da entrada de tráfego deve possuir, ao menos, as seguintes características:

1.8.2.145.1 *DNS* autoritativo.

1.8.2.145.2 *DNS* secundário.

1.8.2.145.3 DNS resolver.

1.8.2.145.4 *DNS* cache.

1.8.2.145.5 Balanceamento de *DNS servers.*

1.8.2.145.6 DNSSec.

1.8.2.146 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.*

1.8.2.147 A solução deve realizar o *offload* dos servidores de *DNS*, funcionando como o *DNS* secundário;

1.8.2.148 A solução deve suportar pelo menos os seguintes tipos de requisição *DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT.*

1.8.2.149 Deve ser capaz de gerar estatísticas sobre consultas de *DNS* por: Aplicação, nome da *query*, tipo da *query*, endereço IP do cliente.

1.8.2.150 Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura.

1.8.2.151 Deve prover as respostas a *queries DNS* da própria *RAM CACHE.*

1.8.2.152 A solução deve ser capaz de realizar *IP Anycast.*

1.8.2.153 A solução deve ser capaz de realizar *DNSSec*, independente da estrutura dos servidores DNS em uso.

1.8.2.154 A solução de alta disponibilidade não deve depender de *BGP* ou outro protocolo de roteamento.

1.8.2.155 Suportar pelo menos os seguintes algoritmos de balanceamento:

1.8.2.155.1 Round Robin.

1.8.2.155.2 Global Availability.

1.8.2.155.3 Ratio.

1.8.2.155.4 LDNS Persist.

1.8.2.155.5 Geografia.

1.8.2.155.6 Disponibilidade da Aplicação.

1.8.2.155.7 Capacidade do Virtual Server.

1.8.2.155.8 Least Connections.

1.8.2.155.9 Pacotes por segundo.

1.8.2.155.10 Round trip time.

1.8.2.155.11 Hops.

1.8.2.155.12 Packet Completion Rate.

1.8.2.155.13 QoS definido pelo usuário.

1.8.2.155.14 Kilobytes per Second.

1.8.2.156 A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (*requests AAAA ou A6*).

1.8.2.157 A solução deve suportar *edns-client-subnet* (ECS) para tanto responder requisições de clientes ou encaminhar requisições de clientes (*screening*).

1.8.2.158 Baseado no *ECS DNS* deve ser possível preservar o endereço IP da *subnet* do cliente ao invés do *LDNS* para tomar decisões.

1.8.2.159 A solução deve funcionar pelo menos das seguintes formas:

1.8.2.159.1 Usar o *ECS* para tomar decisões baseado em topologia (*Subnets*).

1.8.2.159.2 Injetar o *ECS (proxy requests*) para outros servidores *DNS*.

1.8.2.160 A solução deve fazer persistência baseado no endereço IP do cliente (*ECS*), significando que se o cliente mudar de *LDNS* resolver (suporte *ECS*).

1.8.2.161 Possuir recursos para executar compressão de conteúdo *HTTP*, para reduzir a quantidade de informações enviadas ao cliente.

1.8.2.162 Definir qual tipo de compressão será habilitada (*gzip1 a gzip9, deflate*).

1.8.2.163 Possuir capacidade para definir compressão especificamente para certos tipos de objetos.

1.8.2.164 Permitir o balanceamento de aplicações em um pool de servidores, independentemente do hardware, sistema operacional e tipo de aplicação.

1.8.2.165 Suportar os seguintes métodos de balanceamento:

1.8.2.165.1 Round Robin.

1.8.2.165.2 Least Connection.

1.8.2.165.3 Por peso.

1.8.2.165.4 Servidor ou equipamento com resposta mais rápida baseado no tráfego real.

1.8.2.165.5 *Weighted Percentage* dinâmico (baseado no número de conexões).

1.8.2.166 Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI.

1.8.2.167 A solução deve permitir aplicar criptografia de *cookies* para a proteção dos *cookies* utilizados pela aplicação web.

1.8.2.168 Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

1.8.2.168.1 Por *cookie.*

1.8.2.168.2 Endereço de origem.

1.8.2.168.3 Sessão *SSL.*

1.8.2.168.4 Análise da URL acessada.

1.8.2.168.5 Através de qualquer parâmetro do cabeçalho HTTP.

1.8.2.168.6 Através da análise do *MS Terminal Services Session (MSRDP).*

1.8.2.168.7 Através da análise do *SIP Call ID ou Source IP.*

1.8.2.168.8 Através da análise de qualquer informação da porção de dados (camada 7).

1.8.2.169 O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:

1.8.2.169.1 ICMP, TCP, HTTP, HTTPs.

1.8.2.169.2 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.

1.8.2.170 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor.

1.8.2.171 Realizar *Network Address Translation (NAT)*.

1.8.2.172 Realizar proteção contra *syn flood.*

1.8.2.173 Realizar as proteções de cabeçalho: *X-Frame-Options, X-XSS-Protection, X-Content- Type- Options.*

1.8.2.174 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 atividades maliciosas ou ataques de rede.

1.8.2.175 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.

1.8.2.176 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.

1.8.2.177 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.

1.8.2.178 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.

1.8.2.179 A solução deve utilizar *Cache Array Routing Protocol (CARP)* no algoritmo de *HASH.*

1.8.2.180 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real.

1.8.2.181 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual.

1.8.2.182 Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores.

1.8.2.183 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico.

1.8.2.184 Realizar *Network Address Translation (NAT)*.

1.8.2.185 Realizar Proteção contra *Denial of Service (DoS).*

1.8.2.186 Realizar Proteção contra *Syn flood*.

1.8.2.187 Realizar Limpeza de cabeçalho *HTTP*.

1.8.2.188 Deve possuir suporte a *Link Layer Discovery Protocol (LLDP)*.

1.8.2.189 Deve ser possível enviar, pelo menos, as seguintes informações via *LLDP*:

1.8.2.189.1 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.

1.8.2.190 Suporte a otimização do protocolo *TCP* para ajustes a parâmetros das conexões clientes e servidor.

1.8.2.191 Deve ser capaz de realizar *DHCP relay.*

1.8.2.192 Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:

1.8.2.192.1 Tempo de resposta da aplicação;

1.8.2.192.2 Latência;

1.8.2.192.3 Conexões para conjunto de servidores, servidores individuais;

1.8.2.192.4 Por *URL*;

1.8.2.192.5 A solução deve ter suporte a TLS 1.3.

1.9 DE PROJETO E DE IMPLEMENTAÇÃO

1.9.1 Não se aplica.

1.10 DE IMPLANTAÇÃO

1.10.1 O serviço de implantação poderá ser executado presencialmente na Sede do Tribunal Regional Eleitoral do Rio Grande do Norte ou remotamente, acompanhados e supervisionados por sua equipe técnica e realizados prioritariamente durante o expediente normal da Justiça Eleitoral do Rio Grande do Norte.

1.10.1.1 Caso necessário, visando minimizar o impacto para os usuários, o Tribunal Regional Eleitoral do Rio Grande do Norte poderá exigir a execução da implantação fora do horário de expediente normal.

1.10.2 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 do TRE/RN.

1.10.3 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 para a contratação.

1.11 DE GARANTIA E MANUTENÇÃO

1.11.1 A garantia técnica compreenderá todas as funcionalidades da solução ofertada e, também, nas descritas nos manuais e demais documentos técnicos, incluindo a atualização de versões de *software*.

1.11.2 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 TRE/RN.

1.11.3 A fornecedora da solução deverá apresentar ao TRE/RN, antes do início da vigência do serviço de garantia técnica, todos os dados necessários para o registro de chamados técnicos na sua Central de Atendimento, tais como, e-mail, números de telefone e fax, etc.

1.11.3.1 A fornecedora da solução 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 por todo o período da garantia técnica.

1.11.4 Suporte Técnico durante o período de Garantia Técnica:

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

1.11.4.2 A fornecedora da solução 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 TRE/RN, o direito de exigir a atualização sem que isso implique acréscimo aos preços contratados.

1.11.4.3 A manutenção corretiva será realizada em período integral, 07 (sete) dias por semana e 24 (vinte e quatro) horas por dia, após solicitação do TRE/RN.

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

1.11.6 O TRE/RN poderá realizar a aplicação de pacotes de correção e migração de versões e *releases* das licenças de *software*, quando lhe for conveniente, cabendo à fornecedora da solução orientar e colocar à disposição um técnico para contato em caso de dúvidas ou falhas.

1.11.6.1 O TRE/RN reserva-se o direito de proceder a outras configurações, instalações ou conexões nos equipamentos, desde que tal iniciativa não implique em danos físicos e lógicos aos equipamentos, sem que isto possa ser usado como pretexto pela Contratada para se desobrigar do suporte da solução.

1.11.7 A fornecedora da solução 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.

1.11.8 A fornecedora da solução 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.

1.11.9 O serviço de garantia técnica deverá permitir o acesso do TRE/RN 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.

1.11.10 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.

1.11.11 Quando a garantia técnica for acionada, o atendimento deverá ser iniciado imediatamente, independente do meio utilizado.

1.11.12 A fornecedora da solução deverá conceder acesso ao TRE/RN ao controle de atendimento para

acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do Gestor do Contrato.

1.12 DE CAPACITAÇÃO

1.12.1 Deverá ser realizado o repasse tecnológico para a equipe técnica por meio presencial ou remotamente, e deverá abordar as informações necessárias à gerência, administração, auditoria e suporte interno da solução.

1.12.2 Além do repasse tecnológico para as equipes técnicas, deverão ser fornecidos documentos e tutoriais (em português) necessários à capacitação dos usurários finais a respeito das funcionalidades da solução.

1.13 DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE QUE PROJETARÁ, IMPLEMENTARÁ E IMPLANTARÁ A SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

1.13.1 Os serviços previstos objeto deste estudo preliminar deverão ser realizados por profissionais com perfis técnicos compatíveis com cada atividade, ou seja, por recursos especialistas habilitados, com base em cursos e certificações oficiais.

1.13.2 Para esta solução será necessária a capacitação do corpo técnico e implementação com acompanhamento de um profissional especializado na solução e/ou pelo próprio fabricante, por se tratar de uma solução complexa.

1.13.3 A fornecedora da solução deverá possuir pelo menos 01 (um) profissional capacitado com certificação, e deverá apresentar certificado técnico da solução durante a fase de habilitação.

1.13.4 Os profissionais que inicialmente manterão relacionamento direto com o TRE/RN deverão ser apresentados após assinatura do CONTRATO na REUNIÃO INICIAL, ocasião em que deverão ser entregues as comprovações dos perfis exigidos.

1.13.4.1 A apresentação de novos profissionais durante a execução da contratação, incluindo a entrega das comprovações dos perfis à equipe de fiscalização da contratação, deverá ser feita previamente ao início da atuação destes.

1.14 DE FORMAÇÃO DA EQUIPE QUE PROJETARÁ, IMPLEMENTARÁ E IMPLANTARÁ A SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

1.14.1 Não se aplica.

1.15 DE METODOLOGIA DE TRABALHO

1.15.1 Não se aplica.

1.16 DE SEGURANÇA DA INFORMAÇÃO

1.16.1 A fornecedora da solução deverá obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pela JUSTIÇA ELEITORAL e, em especial, observar a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, instituída através da Resolução no 23.501 de 19 de dezembro de 2016 do Tribunal Superior Eleitoral e a Política de Segurança da Informação (PSI), no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte, instituída através da Resolução n° 20/2019 de 11 de setembro de 2019, quanto aos seguintes aspectos:

1.16.1.1 Manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Rio Grande do Norte aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa.

1.16.1.2 O Tribunal Regional Eleitoral do Rio Grande do Norte terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação.

1.16.1.3 Os documentos eventualmente produzidos deverão ser repassados ao Tribunal Regional Eleitoral do Rio Grande do Norte tanto em formato não editável (*PDF*) como também em formato editável (*.DOCX* ou *.ODT*).

1.16.2 A fornecedora da solução deverá concordar que as informações a que terá acesso serão utilizadas somente nos processos envolvidos para execução do objeto contratado.

1.16.3 A fornecedora da solução se obriga a informar imediatamente ao Tribunal Regional Eleitoral do Rio Grande do Norte qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

1.16.4 A solução deverá proporcionar a disponibilidade, a integridade e a segurança de todas as informações do Tribunal Regional Eleitoral do Rio Grande do Norte por ela gerenciadas e armazenadas.

1.16.5 O acesso as ferramentas de colaboração e comunicação deverá ser feito através de conexão segura (*HTTPS*).

1.17 DE QUALIDADE

1.17.1 Não se aplica.

2 AVALIAÇÃO DE SOLUÇÕES

2.1 DISPONIBILIDADE DE SOLUÇÃO SIMILAR EM OUTRO ÓRGÃO OU ENTIDADE DA ADMINISTRAÇÃO PÚBLICA

2.1.1 EMPRESA DE TECNOLOGIA E INFORMAÇÕES DA PREVIDÊNCIA – DATAPREV – Registro de preços para aquisição de até 58 (cinquenta e oito) equipamentos (*Appliance*) de controle de entrega de aplicação (*Application Delivery Controller – ADC*), Balanceador Global (balanceamento de sites) e *Firewall de Aplicação Web (WAF – Web Application Firewall)* de *hardware* e software destinados ao *Datacenter*, com garantia de 60 (sessenta) meses. PREGÃO ELETRÔNICO No 2019/ 01355.

2.1.2 TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO – Solução de Balanceadores de Carga de aplicação para a implantação nos perímetros de usuário e de *DataCenter*, de modo a permitir, entre outras funções, o balanceamento de carga entre as aplicações, além de fornecer mecanismos de segurança mais específicos, incluindo, equipamentos físicos, solução de gerenciamento da solução, serviço de implantação/migração, treinamento, suporte técnico, suporte técnico especializado (sob demanda), pelo prazo de 51 (cinquenta e um) meses, conforme Anexo IA (Complementação ao Termo de Referência) e, conforme especificado no termo de referência (ANEXOI). PREGÃO ELETRÔNICO N° 0046/2021.

2.1.3 TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO SUL – Contratação de empresa especializada no fornecimento, instalação e configuração de sistema de balanceamento de carga de aplicações com *firewall* de aplicação integrado, incluindo testes operacionais, operação assistida e demais componentes necessários ao seu perfeito funcionamento, bem como os serviços de migração, treinamento, garantia e de suporte técnico. PREGÃO ELETRÔNICO Nº 198/2019.

2.1.4 TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO – Registro de preços para eventual aquisição de Solução de Segurança da Informação – Controle de Aplicação com assistência técnica da garantia de 60 (sessenta) meses, compreendendo os serviços de Implantação da Solução, Operação Assistida, Treinamentos e Consultoria Técnica. PREGÃO ELETRÔNICO SRP N° 41/2016.

2.1.5 TRIBUNAL DE CONTAS DO ESTADO DO AMAPÁ – Contratação de empresa especializada para o fornecimento de Solução integrada de segurança, composta por um *cluster* de Gerenciamento Unificado de Ameaças (*Firewall UTM*) e seu Gerenciamento de Logs e Relatórios de Segurança; Solução em *Firewall* de Aplicações *WEB (WAF – Web Application Firewall).* PREGÃO ELETRÔNICO Nº 01/2021.

2.2 DISPONIBILIDADE SOLUÇÕES EXISTENTES NO PORTAL DO *SOFTWARE* PÚBLICO BRASILEIRO

2.2.1 Não há solução deste tipo que atenda os requisitos funcionais e técnicos.

2.3 CAPACIDADE E ALTERNATIVAS NO MERCADO DE TIC, INCLUSIVE A EXISTÊNCIA DE *SOFTWARE* LIVRE OU *SOFTWARE* PÚBLICO

2.3.1 Alternativas de soluções presentes no mercado de TIC:

2.3.1.1 *Imperva Cloud WAF*.

2.3.1.2 *Radware*.

2.3.1.3 F5.

2.3.1.4 Barracuda.

2.3.1.5 *Akamai*.

2.3.2 Alternativas de soluções de software livre:

2.3.2.1 *ModSecurity* da *TrustWave*.

2.3.2.2 *Ironbee*.

2.4 OBSERVÂNCIA ÀS POLÍTICAS, PREMISSAS E ESPECIFICAÇÕES TÉCNICAS DEFINIDAS PELOS MODELO NACIONAL DE INTEROPERABILIDADE DO PODER JUDICIÁRIO (MNI) E MODELO DE ACESSIBILIDADE DE GOVERNO ELETRÔNICO (E-MAG)

2.4.1 A solução a ser implantada não tem por finalidade a comunicação com outros órgãos do Poder Judiciário, portanto, não se aplica a observância ao Modelo Nacional de Interoperabilidade MNI.

2.4.2 A solução a ser implantada será acessível somente a determinados servidores do quadro deste Regional, portanto, não se aplica a observância ao Modelo de Acessibilidade de Governo Eletrônico E-MAG.

2.5 OBSERVÂNCIA AOS REQUISITOS ESTABELECIDOS PELA RESOLUÇÃO CNJ Nº 211/2015 E ALTERAÇÕES POSTERIORES, NA CONTRATAÇÃO DE SERVIÇOS DE DESENVOLVIMENTO E DE SUSTENTAÇÃO DE SISTEMAS DE INFORMAÇÃO

2.5.1 Não se aplica.

2.6 ADERÊNCIA ÀS REGULAMENTAÇÕES DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS (ICP-BRASIL), QUANDO HOUVER NECESSIDADE DE UTILIZAÇÃO DE CERTIFICADO DIGITAL, OBSERVADA A LEGISLAÇÃO SOBRE O ASSUNTO

2.6.1 Não se aplica.

2.7 OBSERVÂNCIA ÀS ORIENTAÇÕES, PREMISSAS E ESPECIFICAÇÕES TÉCNICAS E FUNCIONAIS DEFINIDAS PELO MODELO DE REQUISITOS PARA SISTEMAS INFORMATIZADOS DE GESTÃO DE PROCESSOS E DOCUMENTOS DO PODER JUDICIÁRIO (MOREQ-JUS), DO CONSELHO NACIONAL DE JUSTIÇA – CNJ E PELO E-ARQ (NORMAS E PADRÕES DE ARQUIVOLOGIA)

2.7.1 Não se aplica.

2.8 ORÇAMENTO ESTIMADO QUE EXPRESSE A COMPOSIÇÃO DE TODOS OS CUSTOS UNITÁRIOS RESULTANTES DOS ITENS A SEREM CONTRATADOS, ELABORADO COM BASE EM PESQUISA FUNDAMENTADA DE PREÇOS, COMO OS PRATICADOS NO MERCADO DE TIC EM CONTRATAÇÕES SIMILARES REALIZADAS POR ÓRGÃOS OU ENTIDADES DA ADMINISTRAÇÃO PÚBLICA, ENTRE OUTROS PERTINENTES

2.8.1 Em consulta realizada para uma prévia comparação de custos, se obteve o seguinte cenário caso a solução adquirida seja um *Appliance* Físico:

Item	Descrição	Quantidade	Preço 60 (sessenta) meses R$	Preço Total R$
1	Solução de *Web Application Firewall* e Balanceamento de Carga – *Appliance* Físico	2	825.337,50	1.650.675,00
2	Serviço de instalação e configuração	1	45.208,15	45.208,15
3	Treinamento Especializado	5	35.273,17	176.365,85
Total				**1.872.249,00**

2.8.2 Em consulta realizada para uma prévia comparação de custos, se obteve o seguinte cenário caso a solução adquirida seja um *Appliance* Virtual:

Item	Descrição	Quantidade	Preço 60 (sessenta) meses R$	Preço Total R$
1	Solução de *Web Application Firewall* e Balanceamento de Carga – *Appliance* Virtual	2	498.000,00	996.000,00
2	Serviço de instalação e configuração	1	45.208,15	45.208,15
3	Treinamento Especializado	5	35.273,17	176.365,85
Total				**1.217.574,00**

3 ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO

3.1 A solução escolhida foi a alternativa descrita:

3.1.1 As soluções descritas no **item 2.3.1** são as melhores alternativas para compor a escolha a ser adotada, pois além de possuírem vários recursos, contam com uma sólida equipe de suporte especializado para a realização de treinamentos e resolução de problemas técnicos que possam surgir.

3.1.2 É interessante ressaltar que as soluções propostas no **item 2.3.2** não atendem aos requisitos deste estudo pelo fato de não proverem serviços, como treinamentos, suporte especializado para implantação e operação.

3.1.2.1 Além disso, apesar da possibilidade da composição da solução ser factível para Software Livre, as tarefas para integração, implantação e manutenção da solução sobre a equipe de Segurança demandariam elevado tempo até que seja alcançado um nível de proteção minimamente adequado, sendo inclusive inevitável a necessidade de integração de diferentes softwares e soluções, na maioria das vezes, sem a possibilidade de suporte especializado externo.

3.1.2.2 Por contar com um quantitativo de equipe reduzida para a administração da segurança da informação, os tribunais não poderiam contar com o auxílio de contratação de empresas especializadas para solucionar problemas técnicos que poderiam surgir.

3.1.3 Considerando a participação deste Regional em grupo nacional, inicialmente, optou-se pela alternativa que oferecia mais vantajosidade para o Tribunal Regional Eleitoral do Rio Grande do Norte (TRE/RN) que era a de atuar como partícipe da Ata de Registro de Preços (ARP) nº 91/2022 – PROCESSO n.º: 0008981-46.2021.6.14.8000 – TRE/PA, na qual estava a frente o Tribunal Regional Eleitoral do Pará (TRE/PA), onde foi respondida a consulta formalizada neste sentido, sinalizando os itens de interesse e suas respectivas quantidades (registrada por item).

3.1.3.1 A solução indicada foi a de *Web Application Firewall (WAF)* do tipo *Appliance* Físico.

3.1.4 Posteriormente, após análise das soluções apresentadas na Ata de Registro de Preços (ARP) nº 91/2022 – PROCESSO n.º: 0008981-46.2021.6.14.8000 – TRE/PA, observou-se que a solução de *Web Application Firewall (WAF)* do tipo *Appliance* Virtual possuía as mesmas funcionalidades que a solução do tipo *Appliance* Físico, porém com um valor menor e que poderia ser implantada na nossa estrutura de virtualização.

3.2 Justificativa da escolha:

3.2.1 A Ata de Registro de Preços (ARP) nº 91/2022 – PROCESSO n.º: 0008981-46.2021.6.14.8000 – TRE/PA, para a contratação da solução de *Web Application Firewall (WAF),* realizada pelo Tribunal Regional Eleitoral do Pará (TRE/PA), atende a todos os requisitos elencados neste estudo, onde o processo está finalizado e se configuraria a solução mais vantajosa, caso o Tribunal Regional Eleitoral do Rio Grande do Norte (TRE/RN) opte por participar do referido registro de preços.

3.2.1.1 Vale ressaltar que, dos itens oferecidos nesta Ata, a solução composta pelo *Appliance* Virtual é economicamente mais vantajosa, pois além de realizar todas as funcionalidades que o *Appliance* Físico, possui um valor menor e pode ser implantada na nossa estrutura de virtualização.

3.2.2 Esta ata de registro de preços é composta por:

Item	Descrição	Quantidade	Valor Unitário Registrado
1	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL (WAF), DO TIPO APPLIANCE FÍSICO, COM GARANTIA DE 60 (SESSENTA) MESES	28	R$ 826.398,00
2	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL (WAF), DO TIPO APPLIANCE VIRTUAL, COM GARANTIA DE 60 (SESSENTA) MESES	20	R$ 499.573,00
3	CAPACIDADE ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB	28	R$ 120.562,00
4	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	20	R$ 41.036,00
5	TREINAMENTO ESPECIALIZADO	90	R$ 19.625,00
6	SERVIÇO DE OPERAÇÃO ASSISTIDA	19	R$ 23.691,00

3.3 A solução está alinhada:

3.3.1 Às necessidades de negócio e requisitos tecnológicos.

3.3.2 Necessidade de alcance dos seguintes objetivos estratégicos, elencados no:

3.3.2.1 Plano Estratégico da Justiça Eleitoral do RN 2021-2026 (PEJERN):

3.3.2.1.1 Fortalecimento da segurança da informação – Objetivo Estratégico AC3.

3.3.2.1.1.1 Promover o fortalecimento contínuo da segurança da informação no âmbito ins6tucional – Inicia6va AC3.1.

3.3.2.1.1.2 Fortalecer a segurança cibernética assegurando o alinhamento às diretrizes do Poder Judiciário – Iniciativa AC3.2.

3.3.2.1.1.3 Aprimorar a infraestrutura tecnológica e os serviços em nuvem – Iniciativa AC3.3.

3.3.2.1.1.4 Fortalecer a gestão de riscos de incidentes de TIC – Inicia6va AC3.4.

3.3.2.1.1.5 Implementar mecanismos voltados à proteção de dados pessoais – Iniciativa AC3.5.

3.3.2.2 Plano Diretor de Tecnologia da Informação e Comunicação 2021-2022 (PDTIC):

3.3.2.2.1 Aprimorar a segurança da informação e gestão de dados – Objetivo Estratégico OE7 – Camada 1.

3.3.2.2.2 Aprimorar protocolos de cibersegurança – Objetivo Tático OT7.1 – Camada 2.

3.3.2.2.3 Aprimorar controles de segurança e proteção de dados pessoais – Objetivo Tático OT7.2 – Camada 2.

3.3.2.2.4 Promover serviços de infraestrutura e soluções corporativas – Objetivo Estratégico OE8 – Camada 1.

3.3.2.2.5 Prover soluções e serviços de infraestrutura com capacidade, disponibilidade e desempenho adequados – Objetivo Estratégico OT8.2 – Camada 2.

3.4 A solução escolhida permitirá:

3.4.1 Garantir que o acesso lógico aos ativos seja gerenciado e protegido, por meio de mecanismos de segurança de perímetro.

3.4.2 Tornar a infraestrutura da Justiça Eleitoral mais segura e confiável.

3.4.3 Prover resiliência ao ambiente de produção.

3.4.4 Assegurar a redundância adequada ao acesso de Sistemas hospedados pelo Tribunal.

3.5 Os valores estimados estão descritos no item 3.2.2.

3.6 Os benefícios gerados são:

3.6.1 Reduzir os riscos existentes, relacionados à publicação de sistemas informatizados na Internet e Intranet.

3.6.2 Aplicar controles para mitigação de riscos, em conformidade com a norma ABNT NBR ISO/IEC 27005:2019.

3.6.3 Mitigar ataques cibernéticos à infraestrutura Web conhecidos e prevenção de ataques *Zero Day.*

3.6.4 Melhorar a conformidade em relação às normas e boas práticas de Segurança da informação.

3.6.5 Contribuir na eficácia e segurança de Aplicações *Web*.

3.6.6 Padronizar e auditar políticas de segurança da informação, quanto ao acesso a sistemas e informações sensíveis.

3.6.7 Aumentar a eficiência operacional.

3.7 Relação Demanda Prevista x Quantidade de Bens Pretendidos (memória de cálculo):

3.7.1 Atualmente, considerando o aspecto orçamentário, a necessidade será atendida pela contratação de licenças do(s) seguinte(s) *software(s)*, na(s) quantidade(s) indicada(s):

Descrição	Quantidade Atual	Quantidade Necessária (Projeção)	Quantidade para Aquisição
FORNECIMENTO DE SOLUÇÃO DE *WEB APPLICATION FIREWALL (WAF)*, DO TIPO *APPLIANCE* VIRTUAL, COM GARANTIA DE 60 (SESSENTA) MESES.	0	2	2
SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO *HANDS-ON*	0	1	1
TREINAMENTO ESPECIALIZADO	0	5	5

4 NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE

4.1 Não existe necessidade de adequação do ambiente para a execução contratual.

II – SUSTENTAÇÃO DA CONTRATAÇÃO

5 DEFINIÇÃO DE RECURSOS HUMANOS E MATERIAIS

5.1 IDENTIFICAÇÃO DOS RECURSOS HUMANOS NECESSÁRIOS À IMPLANTAÇÃO DA SOLUÇÃO

5.1.1 Representante Técnico na licitação

5.1.1.1 Francisco de Assis Paiva Leal

5.1.1.2 Responsabilidades:

5.1.1.2.1 Apoiar o pregoeiro durante todo processo licitatório

5.1.1.2.2 Responder os questionamentos dos licitantes durante o certame.

5.1.2 Técnico Segurança da Informação

5.1.2.1 Francisco de Assis Paiva Leal.

5.1.2.2 Responsabilidades:

5.1.2.2.1 Analisar se todos requisitos técnicos exigidos foram atendidos durante o processo de entrega da solução.

5.1.2.2.2 Monitorar a solução no estagio de produção.

5.1.2.2.3 Acionar o suporte de garantia quando necessário.

5.1.3 Equipe de Recebimento

5.1.3.1 Seção de Segurança da Informação

5.1.3.2 Responsabilidades:

5.1.3.2.1 Monitorar a entrega da solução quanto ao prazo e os requisitos técnicos e administrativos.

5.2 IDENTIFICAÇÃO DOS RECURSOS MATERIAIS NECESSÁRIOS À IMPLANTAÇÃO DA SOLUÇÃO

5.2.1 Não foi identificada a necessidade de recursos materiais adicionais para garantir a implantação da solução.

5.3 IDENTIFICAÇÃO DOS RECURSOS HUMANOS NECESSÁRIOS À CONTINUIDADE DA SOLUÇÃO

5.3.1 Não foi identificada a necessidade de recursos humanos adicionais para garantir a continuidade da solução.

5.4 IDENTIFICAÇÃO DOS RECURSOS MATERIAIS NECESSÁRIOS À CONTINUIDADE DA SOLUÇÃO

5.4.1 Não foi identificada a necessidade de recursos materiais adicionais para garantir a continuidade da solução.

6 DEFINIÇÃO DAS ATIVIDADES DE TRANSIÇÃO E ENCERRAMENTO DA CONTRATAÇÃO

6.1 Não se aplica.

7 ELABORAÇÃO DE ESTRATÉGIA DE INDEPENDÊNCIA

7.1 TRANSFERÊNCIA DE CONHECIMENTO TECNOLÓGICO

7.1.1 Não se aplica.

7.2 DIREITOS DE PROPRIEDADE INTELECTUAL E AUTORAIS

7.2.1 Não se aplica.

7.3 DOCUMENTAÇÃO E AFINS PERTINENTES À TECNOLOGIA DE CONCEPÇÃO, MANUTENÇÃO, ATUALIZAÇÃO E CÓDIGO FONTE

7.3.1 Não se aplica.

III – ANÁLISE DE RISCOS

8 IDENTIFICAÇÃO DOS RISCOS

8.1 RISCOS DO PROCESSO DE CONTRATAÇÃO

Risco	**8.1.1 Indisponibilidade Orçamentária**	**Probabilidade:**	**MÉDIA**
Item	Dano		Impacto:
1	Não contratação imediata da solução		**ALTO**
2	Atraso no cronograma		**MÉDIO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Verificar e confirmar previamente disponibilidade orçamentária para a contratação da solução pretendida		STIE
2	Encaminhar em tempo hábil proposta de dotação orçamentária ao Órgão Ordenador de Despesas com previsão e prazo para a contratação da solução		STIE
Item	**Corretiva**		**Responsável**
1	Solicitar o remanejamento de recursos para atender temporariamente o serviço objeto do Termo de Referência		STIE

Risco	**8.1.1 Atraso no Trâmite Processual**	**Probabilidade:**	**MÉDIA**
Item	**Dano**		**Impacto:**
1	Atraso na contratação da solução		**MÉDIO**
2	Atraso no cronograma		**MÉDIO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Finalizar o Termo de Referência e documentos acessórios respeitando o cronograma previamente definido		Equipe de Planejamento da Contratação
2	Comunicar à Administração da criticidade do objeto contratado e da necessidade de agilidade na análise dos documentos e na tramitação do processo administrativo		STIE
Item	**Corretiva**		**Responsável**
1	Comunicar à Administração sobre a paralisação do processo durante a tramitação e solicitar prioridade na análise visando à conclusão do processo administrativo		STIE

Risco	8.1.2 Impugnação Procedente	Probabilidade:	BAIXA
Item	**Dano**		**Impacto:**
1	Interrupção do processo de contratação		**ALTO**
2	Atraso no cronograma		**ALTO**
3	Frustração da contratação		**ALTO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Elaboração de Estudos Preliminares e Termo de Referências consistentes que permitam assegurar a contratação		Equipe de Planejamento da Contratação
2	Revisar o Termo de Referência e certificar que o mesmo não possua cláusulas que restrinjam, sem a devida justificativa técnica, a participação de interessados ou que, de alguma forma, deixem um licitante em situação privilegiada para concorrer		Equipe de Planejamento da Contratação
3	Submeter, para análise, o Termo de Referência à Administração		Equipe de Planejamento da Contratação
4	Atendimento imediato por parte do suporte técnico a fim de responder, tempestivamente, os pedidos de esclarecimentos e impugnações apresentadas		Equipe de Planejamento da Contratação
Item	**Corretiva**		**Responsável**
1	Adequação do Termo de Referência, corrigindo os itens que foram motivos de impugnação, para viabilizar a reabertura do certame.		Equipe de Planejamento da Contratação
2	Promover a reabertura da licitação		Área Administrativa

Risco	8.1.3 Licitação Frustrada (Deserta/Fracassada)	Probabilidade:	BAIXA
Item	**Dano**		**Impacto:**
1	Interrupção do processo de contratação		**ALTO**
2	Atraso no cronograma		**ALTO**
3	Frustração da contratação		**ALTO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Promover análise de mercado com o objetivo de elencar as empresas que prestam serviço do objeto		Equipe de Planejamento da Contratação
2	Dar a devida publicidade ao certame licitatório		Área Administrativa
3	Evitar exigências técnicas demasiadamente restritivas e desnecessárias		Equipe de Planejamento da Contratação
4	Mensurar o preço global do serviço a ser contratado através de estudo minucioso, com pesquisa de preços na Internet, bem como com prestadores de serviço do ramo		Equipe de Planejamento da Contratação
Item	**Corretiva**		**Responsável**
1	Adequação do Termo de Referência para a realização de novo certame		Equipe de Planejamento da Contratação
2	Promover nova licitação		Área Administrativa
3	Pesquisa de Preços, caso necessário		Equipe de Planejamento da Contratação
4	Contratação Direta		Área Administrativa

Risco	8.1.4 Licitação Anulada	Probabilidade:	BAIXA
Item	**Dano**		**Impacto:**
1	Interrupção do processo de contratação		**ALTO**
2	Atraso no cronograma		**ALTO**
3	Frustração da contratação		**ALTO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Na elaboração do Termo de Referência observar se não existe vício de legalidade		Equipe de Planejamento da Contratação
2	Observar adequada publicidade da licitação		Área Administrativa
Item	**Corretiva**		**Responsável**
1	Adequação das exigências normativas sobre o objeto/procedimento licitatório		Equipe de Planejamento da Contratação
2	Promover a publicidade adequada à modalidade de licitação escolhida		Área Administrativa

8.2 RISCOS DA SOLUÇÃO DE TID (GESTÃO E EXECUÇÃO CONTRATUAL)

Risco	**8.2.1 Solução considerada inadequada pela área requisitante**	**Probabilidade:**	**BAIXA**
Item	**Dano**		**Impacto:**
1	Insatisfação dos usuários dos serviços de TIC		**ALTO**
2	Não utilização da solução		**ALTO**
3	Necessidade de nova avaliação da solução		**MÉDIO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Envolver o usuário/unidade requisitante na participação em todas as fases da contratação		STIE e SAOF
2	Nomear servidores experientes e capacitados para executar a fase de levantamento de requisitos da solução de TIC		STIE
Item	**Corretiva**		**Responsável**
1	Nomear nova Equipe de Planejamento da Contratação, substituindo a atual, para a elaboração de novo Termo de Referência visando a contratação de solução de TIC adequada a solicitação da área demandante		Área Administrativa
2	Nomear equipe ou realocar servidores do Tribunal Regional Eleitoral do Rio Grande do Norte com o objetivo de auxiliar ou assumir, provisoriamente, a operação dos serviços prestados pela equipe da fornecedora da solução		STIE
3	Refazer o levantamento de requisitos junto ao usuário/unidade requisitante		STIE
4	Proceder com as alterações necessárias, na medida do possível, na solução de TIC fornecedora da solução, com objetivo de readequar e reimplantar a solução		STIE

Risco	8.2.2 Não cumprimento do prazo de entrega da solução	Probabilidade:	BAIXA
Item	Dano		Impacto:
1	Atraso na instalação da(s) licença(s)		**BAIXO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Consultar as empresas do ramo sobre adequação do prazo de entrega da solução		STIE
2	Acompanhar rigorosamente junto à empresa o andamento da operação de entrega		Área Administrativa
Item	**Corretiva**		**Responsável**
1	Solicitar o fornecedor para a entrega imediata		Área Administrativa
2	Verificar as sanções cabíveis no caso do não cumprimento do prazo de entrega		Área Administrativa

Risco	8.2.2 Entrega da solução incompatível (especificações)	Probabilidade:	BAIXA
Item	Dano		Impacto:
1	Ineficácia na execução dos serviços prestados pelo Órgão		**ALTO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Verificar se o software está de acordo com as especificações mínimas exigidas no ato de entrega para fins de ateste provisório		STIE
Item	**Corretiva**		**Responsável**
1	Solicitar o fornecedor para a substituição do software incompatível		STIE
2	Informar o gestor da contratação sobre problemas contratuais de garantia		STIE

IV – CONCLUSÃO DOS ESTUDOS PRELIMINARES

9 DECLARAÇÃO DE VIABILIDADE

Em conformidade com o disposto no Manual de Contratações de Tecnologia da Informação e Comunicação, subitem 4.1.1.11, DECLARAMOS a viabilidade da contratação, com base no estudo realizado.

Natal/RN, *(datação eletrônica)*

Equipe de Planejamento da Contratação		
Integrante Demandante	**Integrante Técnico**	**Integrante Administrativo**
(assinado eletronicamente) **Carlos Magno Rozário Câmara** COINF/STIE	(assinado eletronicamente) **Francisco de Assis Paiva Leal** SSI/COINF/STIE	(assinado eletronicamente) **José Jailson da Silva** SEGEC/COLIC/SAOF)