



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

TERMO DE REFERÊNCIA (TR)

1. DESCRIÇÃO DO OBJETO

1.1. OBJETO DA CONTRATAÇÃO

1.1.1. Aquisição de solução de *Web Application Firewall* (WAF), com garantia técnica de 60 (sessenta) meses.

1.2. NATUREZA DO OBJETO

1.2.1. O objeto associado à contratação é considerado comum, nos termos do parágrafo único, do art. 1º, da Lei nº 10.520/2002, c/c art. 4º do Decreto nº 10.024/2019, pois apresenta padrões de desempenho e qualidade que podem ser objetivamente definidos por meio de especificações usuais de mercado.

1.3. CLASSIFICAÇÃO DO OBJETO

1.3.1. Classifica-se o objeto da contratação como bens ou serviços de informática, nos termos do Decreto nº 7.174/2010.

1.4. DETALHAMENTO DO OBJETO

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	CATMA T	QTDE.
1	Fornecimento de solução de Web Application Firewall(WAF), do tipo appliance virtual, com garantia de 60(sessenta) meses.	UN	27464	1

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. DA JUSTIFICATIVA

2.1.1. Com o crescimento dos ataques cibernéticos e espionagem virtual aos quais as empresas privadas e os órgãos da administração pública, e notadamente o judiciário, têm sido vítimas, torna-se urgente a adoção de



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

mecanismos de segurança da informação e a utilização de recursos de inspeção e proteção do tráfego de dados que auxiliem, de forma proativa, a prevenção e proteção dos sistemas, ante às vulnerabilidades encontradas em diversos vetores – redes (perímetro), sistemas e aplicativos, servidores de aplicação, e infraestrutura de orquestradores de containers.

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

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

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

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



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

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

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

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

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



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

captura de dados sensíveis e roubo de credenciais, prevenção à atividade de robôs (bots) maliciosos e muito outros tipos de ataques cibernéticos conhecidos.

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

2.2. MOTIVAÇÃO DA CONTRATAÇÃO E NECESSIDADES DE NEGÓCIO

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

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

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

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

2.2.5. Propõe-se, para tanto, a aquisição de Solução de Segurança da Informação – Firewall de Aplicação Web (WAF), visando à segurança e ao bom



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

desempenho das atividades no âmbito desta Justiça Especializada. Conforme exposto, a aquisição fundamenta-se em razão da necessidade de mitigar os inúmeros riscos inerentes aos sistemas informatizados disponibilizados no Portais Internet e Intranet do Tribunal e, conseqüentemente, aumentar a confiabilidade, integridade e a disponibilidade dos serviços oferecidos ao público interno e à sociedade, segundo as melhores práticas do mercado de segurança da informação.

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

- No quesito segurança, pelo oferecimento de uma camada adicional de defesa, protegendo os servidores que hospedam aplicações Web, e executando funções de segurança de proteção dos servidores internos contra ataques por usuários da internet;
- No quesito performance, pela melhoria de acesso às aplicações dos sistemas administrativos e judiciais, através do balanceamento de carga;
- Ampliar o controle de perímetro, por meio da inspeção e análise contínuo de tráfego das aplicações;
- Aprimorar os mecanismos de monitoramento e detecção de ataques;
- Proporcionar a prevenção e mitigação de Ameaças Cibernéticas;
- Contribuir para a redução da superfície de ataques cibernéticos da justiça eleitoral.

2.3. BENEFÍCIOS ESPERADOS

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

2.3.2. Tornar a infraestrutura da Justiça Eleitoral mais segura e confiável;

2.3.3. Prover resiliência ao ambiente de produção;

2.3.4. Assegurar a redundância adequada ao porte do parque tecnológico do Regional.

2.4. OBJETIVO DA CONTRATAÇÃO

2.4.1. Trata-se de contratação de empresa para fornecimento de solução de Web Application Firewall (WAF), na modalidade de Appliance Virtual, com garantia técnica de 60 (sessenta) meses, no intuito de criar redundância da solução já adquirida pelo TRE-AM (Contrato nº 44/2022), com a configuração em alta disponibilidade.



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

2.5. ALINHAMENTO ESTRATÉGICO

I - PEI do TRE-AM - Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados.

- Índice de atendimento de demandas e desenvolvimento da área de TIC.

II - PETIC do TRE-AM

- Objetivos Estratégicos de TIC:
 - Prover e aprimorar infraestrutura para os serviços de TIC
 - Aperfeiçoar a gestão de TIC
 - Atendimento às normas vigentes do âmbito da Justiça eleitoral e poder judiciário

III - Outros Referenciais Estratégicos

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

2.6. REFERÊNCIAS AOS ESTUDOS PRELIMINARES

- Processo Administrativo Digital nº 5836/2022.

2.7. REFERÊNCIAS LEGAIS

- Resolução CNJ Nº 182/2013, dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ);



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

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

2.9. RELAÇÃO ENTRE A DEMANDA PREVISTA E A QUANTIDADE A SER CONTRATADA

2.9.1. Conforme mencionado no item 2.4, a contratação ora pretendida tem por objetivo criar redundância da solução já adquirida pelo TRE-AM (Contrato nº 44/2022), com a configuração em alta disponibilidade, assegurando a proteção de aplicações WEB e informações sensíveis armazenadas nos servidores em produção do TRE-AM. Para tanto, devido a necessidade da contratação, foram definidos em Estudo Técnico Preliminar os seguintes itens e respectivas quantidades:

DEMANDA EXISTE	DESCRIÇÃO DA SOLUÇÃO DE TI A SER CONTRATADA	QTDE	JUSTIFICATIVAS
----------------	---	------	----------------



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

Proteção de aplicações web publicadas na internet/intranet, hospedadas no data center do Tribunal Regional Eleitoral do Amazonas.	Cluster/solução de proteção camada 7 para aplicações web, firewall (WAF) do tipo appliance virtual.	1	Cluster de proteção das aplicações WEB hospedadas no ambiente de produção (Data Center) do Tribunal, visando mitigar os riscos de ataque cibernético, com Garantia e suporte técnico do fabricante pelo período de 60(sessenta) meses, necessários à manutenção da disponibilidade da solução.
---	---	---	--

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

3. ESPECIFICAÇÃO TÉCNICA

3.1. REQUISITOS MÍNIMOS DA SOLUÇÃO DE WAF:

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

3.1.2. A solução deverá ser do tipo Appliance Virtual, compatível com os virtualizadores hypervisor VMWARE ESXi 6.5+, KVM., Hyper-V e Acrópolis (Nutanix);

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

3.1.4. 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);

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

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



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

- 3.1.7. Admitir no mínimo 900 (novecentas) transações por segundo (TPS) SSL com chaves RSA 2048 bits;
- 3.1.8. Suportar 2.000.000 (dois milhões) de conexões concorrentes em camada 4;
- 3.1.9. Suportar e garantir a instalação em ambiente de alta disponibilidade;
- 3.1.10. Deve permitir a configuração da solução em alta disponibilidade, permitindo o funcionamento em cluster do tipo ativo-passivo e ativo-ativo.
- 3.1.11. 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.
- 3.1.12. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime" e queda de sessões em caso de falha de uma das unidades.
- 3.1.13. 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.
- 3.1.14. O equipamento deve permitir a sincronização das configurações de forma automática.
- 3.1.15. Caso seja necessária uma interligação entre os equipamentos, a CONTRATADA será integralmente responsável por tal interligação, garantindo a performance necessária para o atendimento da solução.
- 3.1.16. 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;
- 3.1.17. Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, WAF, etc.
- 3.1.18. Fornecer recurso para o transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;
- 3.1.19. Analisar e proteger tráfego HTTP/1.0, HTTP/1.1, HTTP/2.0 e HTTP/3;
- 3.1.20. Possuir suporte a IPv6;
- 3.1.21. 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;
- 3.1.22. Deve suportar, no mínimo, 1000 VLANs simultaneamente;
- 3.1.23. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

- 3.1.24. Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).
- 3.1.25. Assinar cookies digitalmente e editar endereços de URL ("URL Rewriting");
- 3.1.26. O equipamento deverá permitir a sincronização das configurações:
- a) De forma automática;
 - b) Manualmente, forçando a sincronização apenas no momento desejado;
- 3.1.27. Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:
- a) Compartilhar a rede de heartbeat com a rede de dados;
 - b) Utilizar uma rede exclusiva para o heartbeat.
- 3.1.28. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;
- 3.1.29. 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.
- 3.1.30. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.
- 3.1.31. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:
- 3.1.32. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version
- 3.1.33. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.
- 3.1.34. Deve implementar configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para a interface de gerenciamento
- 3.1.35. Permitir acesso in-band via SSH
- 3.1.36. Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.
- 3.1.37. Possuir console de administração com interface gráfica remota segura atendendo os seguintes requisitos:
- a) Permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e logs;



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

- b) Permitir a replicação de configurações e a aplicação de atualização de softwares para os elementos dos nós do cluster;
- 3.1.38. Manter internamente múltiplos arquivos de configurações do sistema;
- 3.1.39. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;
- 3.1.40. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;
- 3.1.41. Deverá ser possível associar aos usuários de bases externas como RADIUS, LDAP e TACACS+ o nível de acesso;
- 3.1.42. Possuir Interface Gráfica via Web;
- 3.1.43. Possuir auto-complementação de comandos na CLI;
- 3.1.44. Possuir ajuda contextual;
- 3.1.45. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;
- 3.1.46. A Solução deve ter suporte a sFlow;
- 3.1.47. Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;
- 3.1.48. Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;
- 3.1.49. A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;
- 3.1.50. A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;
- 3.1.51. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);
- 3.1.52. Suportar a rollback de configuração e imagem;
- 3.1.53. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;
- 3.1.54. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;
- 3.1.55. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;
- 3.1.56. A interface Gráfica deverá permitir a reinicialização do equipamento;
- 3.1.57. Reinicialização do equipamento por comando na CLI;
- 3.1.58. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;
- 3.1.59. Possuir traps SNMP;
- 3.1.60. Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events;



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

- 3.1.61. Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;
- 3.1.62. Implementar Debugging: CLI via console e SSH;
- 3.1.63. Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
- 3.1.64. Permitir a criação de políticas diferenciadas por aplicação.
- 3.1.65. Deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;
- 3.1.66. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
- 3.1.67. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;
- 3.1.68. Permitir as seguintes opções de implementação:
- 3.1.69. Monitoramento (sem bloqueio);
- 3.1.70. Proxy (reverso e transparente).
- 3.1.71. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;
- 3.1.72. Remover as mensagens de erro do conteúdo que será enviado aos usuários;
- 3.1.73. Em modo “monitoramento” (sem bloqueio), realizar análise e avaliação do tráfego, gerar relatórios com os dados analisados e simular bloqueios para efeito de avaliação;
- 3.1.74. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos;
- 3.1.75. Bloquear ataques aos servidores de aplicação, por meio dos seguintes recursos:
 - a) Identificação, isolamento e bloqueio de ataques sofisticados sem impactar nas transações das aplicações;
- 3.1.76. Possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;
- 3.1.77. A solução deve suportar e fazer a proteção do tráfego de protocolo WebSocket.
- 3.1.78. A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automática;
- 3.1.79. 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;



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

- 3.1.80. Quando detectada uma tentativa de ataque bloquear de imediato o tráfego ou a sessão;
- 3.1.81. Bloqueio com intermediação e interrupção da conexão;
- 3.1.82. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;
- 3.1.83. Utilização de página HTML informativa e personalizável como HTTP Response aos bloqueios;
- 3.1.84. Configuração de políticas de bloqueio baseadas em requisição HTTP, endereço IP e usuário de aplicação;
- 3.1.85. Permitir apenas transações de aplicações validadas, o restante das transações deverá ser bloqueado, utilizando bloqueio por nível de aplicação baseado no contexto da sessão do usuário, com privilégios de autorização diferentes, entradas de usuários e tempo de resposta de aplicação;
- 3.1.86. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:
- a) Endereços IP que originaram os ataques;
 - b) Horário do ataque;
 - c) Nome do ataque;
 - d) Qual campo foi atacado;
 - e) Quantas vezes esse ataque foi realizado;
- 3.1.87. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório), cookies, ações SOAP e elementos XML; identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP;
- 3.1.88. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
- 3.1.89. Identificar ataques baseados em:
- a) Assinaturas, com atualização diária da base pelo fabricante;
 - b) Regras;
 - c) Perfis de utilização;
- 3.1.90. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado.
- 3.1.91. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser auto-ajustáveis e adaptativos de acordo com mudanças.



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

3.1.92. A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador.

3.1.93. Detectar ataques de força bruta por meio dos seguintes métodos:

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

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

3.1.96. Detectar ataques do tipo força bruta em que:

- a) O atacante solicita repetidamente o mesmo recurso;
- b) O atacante realiza repetidas tentativas não autorizadas de acesso;
- c) São utilizados ataques automatizados de login.

3.1.97. Detectar ataques do tipo força bruta que explorem:

- a) Controles de acesso da aplicação (Erro 401 – Unauthorized);
- b) Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação;
- c) Aplicações WEB que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação);
- d) Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um range de Ips);
- e) Clientes automatizados (robôs, requisições muito rápidas);
- f) Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
- g) 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;
- h) Possibilitar atualização de novas assinaturas para ataques conhecidos;

3.1.98. Apresentar proteção contra-ataques, como:

- a) Brute Force Login;
- b) Buffer Overflow;
- c) Cookie Injection;
- d) Cookie Poisoning;
- e) Cross Site Request Forgery (CSRF);
- f) Cross Site Scripting (XSS);
- g) Server Side Request Forgery (SSRF)
- h) Directory Traversal;
- i) Forceful Browsing;
- j) HTTP Denial of Service;
- k) HTTP hidden field manipulation;



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

- l) HTTP request smuggling;
 - m) HTTP Response Splitting;
 - n) Malicious Robots;
 - o) Parameter Tampering;
 - p) Remote File Inclusion Attacks;
 - q) Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI);
 - r) Session Hijacking;
 - s) SQL Injection;
 - t) Web Scraping;
 - u) Web server software and operating system attacks;
 - v) Web Services (XML) attacks;
- 3.1.99. Permitir configurar granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;
- 3.1.100. Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:
- a) Assinatura de ataque;
 - b) Código de response;
 - c) Conteúdo da cookie;
 - d) Conteúdo do cabeçalho;
 - e) Conteúdo do payload;
 - f) Hostname;
 - g) IP de origem;
 - h) Método HTTP;
 - i) Número de ocorrências em determinado intervalo de tempo;
 - j) Parâmetro;
 - k) User-agent (navegador);
- 3.1.101. Permitir a criação de assinaturas de ataques.
- 3.1.102. Reconhecer assinaturas seletivas, e filtros de ataque que devem proteger contra:
- a) Ataques de negação de serviços automatizados;
 - b) Worms e vulnerabilidades conhecidas;
 - c) Requests em objetos restritos;
- 3.1.103. Deve proteger contra ataques SSRF (Server Side RequestForgery);
- 3.1.104. A solução oferecida deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra.



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

- 3.1.105. Deve possuir um conjunto de assinaturas para cada tipo de tecnologia bem definidos e agrupados. Portanto permitindo selecionar as tecnologias da aplicação (Apache, PHP, Linux, SQL, etc) para automaticamente selecionar o conjunto de assinaturas que se aplica as mesmas;
- 3.1.106. Ao atualizar ou adicionar uma nova assinatura, a solução deve automaticamente colocar essa assinatura em modo “staging” para evitar falsos positivos e não bloquear tráfego válido. Depois de um período a mesma deve automaticamente entrar em modo de bloqueio;
- 3.1.107. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (File Types);
- 3.1.108. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação, ou enviar para inspeção através do protocolo ICAP;
- 3.1.109. Deve possuir uma proteção proativa comportamental contra ataques automatizados por robôs e outras ferramentas de ataque;
- 3.1.110. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação;
- 3.1.111. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual;
- 3.1.112. Possuir método de mitigação de DoS L7 baseado em:
- a) Descarte de todas as requisições de um determinado IP e/ou país suspeito;
 - b) CAPTCHA para suspeitos que ultrapassem os thresholds;
 - c) Defesa proativa contra Bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô;
- 3.1.113. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego, análise de dados e Machine Learning, com o stress do servidor de aplicação para determinar uma condição de DDoS;
- 3.1.114. Aprender o comportamento da aplicação:
- a) Campos, valores, cookies e URLs;
- 3.1.115. Políticas sugeridas somente devem ser aplicadas após um período configurável;
- 3.1.116. 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;
- 3.1.178. Realizar as checagens em todos os tipos de entrada de dados, como URLs, formulários, cookies, campos ocultos e parâmetros, consultas (query), métodos HTTP, elementos XML e ações SOAP;
- 3.1.118. Proteger contra mensagens XML e SOAP malformadas;



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

- 3.1.119. Utilizar o campo HTTP X-Forwarded-For sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com NAT;
- 3.1.120. Remover as mensagens de erro do conteúdo que será enviado aos usuários;
- 3.1.121. Deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão;
- 3.1.122. Deverá permitir o cadastro de robôs que podem acessar a aplicação;
- 3.1.123. Deverá implementar proteção ao JSON (JavaScript Object Notation);
- 3.1.124. Implementar a segurança de *web services*, através dos seguintes métodos:
- a) Criptografar/Decriptografar partes das mensagens SOAP;
 - b) Assinar digitalmente partes das mensagens SOAP;
 - c) Verificação de partes das mensagens SOAP;
- 3.1.125. Deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;
- 3.1.126. Deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;
- 3.1.127. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário. Deve proteger esses dados criptografados de malwares e keyloggers;
- 3.1.128. Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos. Esse nome de parâmetro deve ser mudado constantemente pela ferramenta para dificultar ataques direcionados;
- 3.1.129. Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal;
- 3.1.130. A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas do equipamento;
- 3.1.131. A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros como por exemplo: Trustwave App



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys, Quotium Seeker, HP Webinspect.

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

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

3.1.133. Deverá permitir o agendamento de relatórios a serem entregues por email;

3.1.134. Emitir os seguintes relatórios gráficos por:

- a) Política de segurança;
- b) Tipos de ataques;
- c) Violações;
- d) URL que foram atacadas;
- e) Endereços IP de origem;
- f) Localização geográfica dos endereços IPs de origem;
- g) Severidade;
- h) Código de resposta;
- i) Métodos;
- j) Protocolos;
- k) Sessão;

3.1.135. Permitir a seleção de período para emissão dos relatórios,

3.1.136. Permitir a geração das seguintes informações, por período:

- a) Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;
- b) Informações estatísticas de quantidade de conexões completadas e bloqueadas;
- c) Informações estatísticas de fluxo de tráfego;
- d) Informações estatísticas de quantidade de sessões ou conexões;

3.1.137. Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: HTTP e HTTPS;

3.1.138. Deve possuir capacidade para definir que todo tráfego seja tunelado e permitir a utilização do protocolo padrão HTTPS com SSL como transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento

3.1.139. 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;



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

3.1.140. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL/TLS sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor.

3.1.141. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado

3.1.142. 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:

- a) SSL session cache Timeout;
- b) Session Ticket;
- c) OCSP (Online Certificate Status Protocol) Stapling;
- d) Dynamic Record Sizing;
- e) ALPN (Application Layer Protocol Negotiation);
- f) Perfect Forward Secrecy;

3.1.143. 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:

- a) 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;
- b) 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;
- c) Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;
- d) Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS;
- e) Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS.

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

3.1.145. A solução deve oferecer ferramenta de Portal de Acesso de Usuários que permita que usuários acessem aplicações internas a partir de rede externas,



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

implementando as funcionalidades de Single Sign-on e VPN-SSL, com os seguintes recursos:

- a) 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;
- b) 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;
- c) modo “Network”, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna;
- d) Ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeiram autenticação, fazendo cache das credenciais do usuário e utilizar a credencial correta para cada sistema;

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

3.1.147. Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware ou one-time passcode (OTP); Deve possuir capacidade para realizar proxy reverso com a finalidade de omitir a URI real, promovendo assim o acesso seguro as aplicações web internas;

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

3.1.149. Deve possuir capacidade para realizar verificações e validações no dispositivo do cliente antes de conceder acesso tais como versão do sistema operacional, antivírus instalado, certificados digitais instalados na máquina, firewall ativado;

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

- a) DNS autoritativo;
- b) DNS secundário;
- c) DNS resolver;
- d) DNS cache;
- e) Balanceamento de DNS servers;
- f) DNSSec;

3.1.151. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;

3.1.152. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

- 3.1.153. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT
- 3.1.154. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;
- 3.1.155. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;
- 3.1.156. Deve prover as respostas a queries DNS da própria RAM CACHE
- 3.1.157. A solução deve ser capaz de realizar IP Anycast;
- 3.1.158. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso
- 3.1.159. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;
- 3.1.160. Suportar pelo menos os seguintes algoritmos de balanceamento:
- a) Round Robin;
 - b) Global Availability;
 - c) Ratio;
 - d) LDNS Persist;
 - e) Geografia;
 - f) Disponibilidade da Aplicação;
 - g) Capacidade do Virtual Server;
 - h) Least Connections;
 - i) Pacotes por segundo;
 - j) Round trip time;
 - k) Hops;
 - l) Packet Completion Rate;
 - m) QoS definido pelo usuário;
 - n) Kilobytes per Second;
- 3.1.161. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);
- 3.1.162. A solução deve suportar edns-client-subnet (ECS) para tanto responder requisições de clientes ou encaminhar requisições de clientes (screening).
- 3.1.163. Baseado no ECS DNS deve ser possível preservar o endereço IP da subnet do cliente ao invés do LDNS para tomar decisões
- 3.1.164. A solução deve funcionar pelo menos das seguintes formas:
- a) Usar o ECS para tomar decisões baseado em topologia (Subnets)
 - b) Injetar o ECS (proxy requests) para outros servidores DNS
- 3.1.165. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver (suporte ECS).



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

- 3.1.166. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;
- 3.1.167. Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);
- 3.1.168. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;
- 3.1.169. Permitir o balanceamento de aplicações em um pool de servidores, independentemente do hardware, sistema operacional e tipo de aplicação;
- 3.1.170. Suportar os seguintes métodos de balanceamento:
- a) Round Robin;
 - b) Least Connection;
 - c) Por peso.
 - d) Servidor ou equipamento com resposta mais rápida baseado no tráfego real;
 - e) Weighted Percentage dinâmico (baseado no número de conexões);
 - f) Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;
- 3.1.171. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web.
- 3.1.172. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
- a) Por cookie;
 - b) Endereço de origem;
 - c) Sessão SSL;
 - d) Análise da URL acessada;
 - e) Através de qualquer parâmetro do cabeçalho HTTP;
 - f) Através da análise do MS Terminal Services Session (MSRDP)
 - g) Através da análise do SIP Call ID ou Source IP;
 - h) Através da análise de qualquer informação da porção de dados (camada 7);
- 3.1.173. O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:
- a) 3.1.174.1. ICMP, TCP, HTTP, HTTPS;
 - b) 3.1.174.2. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;
- 3.1.174. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor;



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

- 3.1.175. Realizar Network Address Translation (NAT);
- 3.1.176. Realizar proteção contra syn flood;
- 3.1.177. Realizar as proteções de cabeçalho: X-Frame-Options, X-XSS-Protection, X-Content-Type-Options
- 3.1.178. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;
- 3.1.179. 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.
 - a) 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.
 - b) Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.
- 3.1.180. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço
- 3.1.181. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;
- 3.1.182. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;
- 3.1.183. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;
- 3.1.184. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;
- 3.1.185. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico;
- 3.1.186. Realizar Network Address Translation (NAT);
- 3.1.187. Realizar Proteção contra Denial of Service (DoS);
- 3.1.188. Realizar Proteção contra Syn flood;
- 3.1.189. Realizar Limpeza de cabeçalho HTTP;
- 3.1.190. Deve possuir suporte a Link Layer Discovery Protocol (LLDP);
- 3.1.191. Deve ser possível enviar, pelo menos, as seguintes informações via LLDP:



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

3.1.192. Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size;

3.1.193. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

3.1.194. Deve ser capaz de realizar DHCP relay;

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

- a) Tempo de resposta da aplicação;
- b) Latência;
- e) Conexões para conjunto de servidores, servidores individuais;
- f) Por URL;
- g) A solução deve ter suporte a TLS 1.3.

4. APRESENTAÇÃO DA PROPOSTA

4.1. Não se aplica, uma vez que, na estratégia da contratação, optou-se por adesão a Ata de Registro de Preços.

5. ESTRATÉGIA DA CONTRATAÇÃO

5.1. ADESÃO A ATA DE REGISTRO DE PREÇOS

5.1.1. Após a finalização dos estudos preliminares, a equipe de planejamento da contratação definiu a aquisição da solução de WAF por meio de adesão à Ata de Registro de Preços nº 91/2022, gerenciada pelo Tribunal Regional Eleitoral do Pará. A vantajosidade da adesão pretendida está caracterizada pelas razões doravante expostas:

- a) A aquisição de Solução de Web Application Firewall está em consonância com a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário – ENSEC-PJ;
- b) Após solicitação formulada pelo TRE-AM, o Tribunal Superior Eleitoral disponibilizou orçamento destinado à aquisição de solução de WAF, visando criar redundância da solução anteriormente contratada com a configuração em alta disponibilidade. Considerando que esse orçamento deve ser obrigatoriamente executado no exercício de 2023, iniciar processo licitatório autônomo representa grande risco de inexecução do objeto e perda orçamentária;
- c) A adesão pretendida aumentará o nível de proteção dos sistemas deste Regional frente as vulnerabilidades encontradas em diversos vetores, tais como redes, servidores de aplicação, sistemas e infraestrutura de orquestradores de containers;



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

- d) Os artefatos produzidos pelo órgão gerenciador do certame licitatório estão em consonância com a demanda apresentada;
- e) Em contato com representante da empresa beneficiária da ARP nº 91/2022 TRE-PA, recebemos manifestação positiva quanto à possibilidade fornecimento;
- f) O Pregão Eletrônico nº 46/2022 – TRE-PA, que deu ensejo à ARP nº 91/2022, contou com a participação de diversos TRE. Desse modo, a adesão à referida ARP garante padronização quanto à solução utilizada no âmbito da Justiça Eleitoral, facilitando a troca de informações e cooperação entre os órgãos;
- g) No subitem 5.10 do Termo de Referência anexo ao Edital de Pregão Eletrônico nº 46/2022 – TRE-PA, que deu ensejo à ARP nº 91/2022, consta previsão expressa de possibilidade de adesão pelos Tribunais Regionais Eleitorais.

5.2. DOTAÇÃO ORÇAMENTÁRIA

5.2.1. As despesas para aquisição do objeto deste Termo de Referência correrão por conta da Fonte Orçamentária 1000 – Segurança da Informação/ Elemento de Despesa 44.90 – Investimento.

5.3. CRITÉRIOS SOCIAIS E CULTURAIS

5.3.1. Todos os manuais, guias de instruções e ajuda deverão ser disponibilizados preferencialmente no idioma Português do Brasil - PtBR e fornecidos em meio digital.

5.3.2. O licenciamento deve ser prestado preferencialmente no idioma português do Brasil.

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

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

5.4. CRITÉRIOS DE SEGURANÇA DA INFORMAÇÃO

5.4.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

5.4.2. O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e Termo de Ciência, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos ANEXOS I - TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO e ANEXO II - TERMO DE CIÊNCIA.

6. DEFINIÇÃO DAS OBRIGAÇÕES CONTRATUAIS

6.1. DEFINIÇÃO DAS OBRIGAÇÕES DA CONTRATANTE

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

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

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

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

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

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

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

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

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



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

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

6.2. DEFINIÇÃO DAS OBRIGAÇÕES DA CONTRATADA

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

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

- a) Manter, durante o fornecimento, todas as condições de habilitação e qualificação exigidas na licitação;
- b) Não transferir a outrem, no todo ou em parte, o objeto do contrato a ser firmado.

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

- a) Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste Termo de Referência, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo e prazo de garantia;
- b) Atender aos chamados técnicos no prazo estipulado pela contratante;
- c) Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);
- d) Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência (item 9.2.3), o objeto com avarias ou defeitos;
- e) Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- f) Responsabilizar-se integralmente pelo fiel cumprimento do objeto contratado, prestando todos os esclarecimentos que forem solicitados pela CONTRATANTE, cujas reclamações se obriga a atender.



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

7. EXECUÇÃO DO CONTRATO

7.1. PRAZO DE ENTREGA

7.1.1. A entrega de equipamentos/ licenças e conclusão de serviços deve ocorrer no prazo máximo de 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Fornecimento.

7.1.2. Os prazos de entrega, substituição e reposição admitem prorrogação, mantidas as demais cláusulas da contratação e da nota de empenho que não sofrerem influência dessa prorrogação, sendo assegurada a manutenção do equilíbrio econômico-financeiro da contratação, desde que ocorra um dos motivos previstos nos incisos I a VI do § 1º do Art. 57 da Lei n. 8.666/93, devendo ser requerida por escrito, justificadamente, e apresentada até o último dia do referido prazo.

7.2. LOCAL DE EXECUÇÃO/ENTREGA

7.2.1. Tribunal Regional Eleitoral do Amazonas (Sede), Avenida André Araújo, nº 200, Aleixo, Manaus-AM CEP 69060-000/ Secretaria de Tecnologia da Informação (STI).

7.3. CONDIÇÕES GERAIS DO FORNECIMENTO

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

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

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

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

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



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

8. FORMA DE PAGAMENTO

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

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

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

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

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

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

9. GESTÃO DO CONTRATO

9.1. DA GARANTIA E DO SUPORTE TÉCNICO

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

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



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

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

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

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

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

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

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

9.1.7. Suporte Técnico durante o período de Garantia Técnica:

- a) Durante o período de garantia técnica de 60 (sessenta) meses, a partir do recebimento definitivo da instalação, a Contratada deverá garantir o funcionamento de toda a solução, fornecer atualizações, prestar suporte técnico e atender aos chamados técnicos para manutenção;
- b) A Contratada deverá comunicar formalmente ao Gestor do Contrato a disponibilidade de novas versões e releases das licenças de software e firmwares, reservando-se, à equipe técnica do CONTRATANTE, o direito de exigir a atualização sem que isso implique acréscimo aos preços contratados;



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

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

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

- a) Relação de todos os chamados técnicos ocorridos no mês anterior, incluindo data e hora do início e término do suporte; identificação do problema; criticidades; providências adotadas para o diagnóstico, solução provisória e solução definitiva; data e hora do início e término da solução definitiva; identificação do técnico do CONTRATANTE que solicitou e validou o chamado; identificação do técnico da Contratada responsável pela execução do chamado, bem como outras informações pertinentes;
- b) Cada chamado técnico aberto será avaliado individualmente pelo Gestor do Contrato;
- c) O serviço será considerado recebido pelo Gestor do Contrato quando do fechamento de cada chamado, desde que não reapareçam posteriormente ao fechamento inconformidades técnicas comprovadamente relacionadas ao chamado recebido;
- d) O Gestor do Contrato emitirá a recusa em caso de verificação de impropriedades ou erros impeditivos de recebimento do serviço prestado. A Contratada deverá promover as correções necessárias, conforme diretrizes a serem estabelecidas pelo Gestor do Contrato, sem prejuízo de aplicação de penalidades previstas.

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

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

9.1.11. A Contratada deverá garantir pleno funcionamento dos equipamentos e softwares, bem como atualizações, responsabilizando-se por qualquer



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

componente adicional que for identificado após a contratação, seja por motivos de interoperabilidade, compatibilidade ou quaisquer outros motivos que impeçam o funcionamento efetivo da solução contratada.

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

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

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

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

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

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

9.2. DO RECEBIMENTO PROVISÓRIO E DEFINITIVO

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

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



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

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

9.3. TERMO DE RECEBIMENTO PROVISÓRIO

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

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

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

9.4. TERMO DE RECEBIMENTO DEFINITIVO

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

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

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



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

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

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

9.4. SANÇÕES ADMINISTRATIVAS

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

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

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

- a) Advertência, nas hipóteses de faltas leves, assim entendidas aquelas que não acarretem prejuízos para o TRE/AM;
- b) Multa compensatória de até 10% (dez por cento) sobre o valor global da contratação, na hipótese de recusa em assinar o contrato;
- c) Multa compensatória de até 10% (dez por cento) sobre o valor global da contratação, na hipótese de recusa em receber a Ordem de Fornecimento e/ou de Serviço;



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

d) Multa compensatória de até 10% (dez por cento) sobre o valor global da contratação, na hipótese de inexecução parcial ou total da obrigação.

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

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

Manaus, 04 de julho de 2023.

Equipe de Planejamento da Contratação:

Rubens Antônio Pinto Soares

Chefe do Núcleo de Segurança da Informação
Requisitante/ Integrante Técnico

Mayara Santos Santos

Coordenadora de Infraestrutura
Integrante Administrativa



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

ANEXO I

TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

A Sociedade Empresária _____, CNPJ _____, por intermédio de seu representante legal abaixo assinado, _____, CPF _____, doravante designados simplesmente CONTRATADA e RESPONSÁVEL, se compromete, por intermédio do presente TERMO DE COMPROMISSO, a não divulgar sem autorização, quaisquer Informações Confidenciais (conforme definido abaixo) em relação ao Projeto de “Contratação de solução de *Web Application Firewall* (WAF)”, e de propriedade do Tribunal Regional Eleitoral do Amazonas, CNPJ nº 05.959.999/0001-14, doravante designado TRE-AM, em conformidade com as seguintes cláusulas e condições:

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



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

relativos a perdas e danos que possam advir ao TRE-AM e aos seus usuários;

7. O descumprimento de quaisquer das cláusulas do presente Termo acarretará a responsabilidade civil e criminal de acordo com as leis aplicáveis dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

Gestor do Contrato do TRE-AM:

Representante da Contratada:

Local, UF, de de



TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Infraestrutura de Tecnologia

ANEXO II

TERMO DE CIÊNCIA

IDENTIFICAÇÃO DO CONTRATO

CONTRATO N°:

OBJETO: “Aquisição de solução de *Web Application Firewall* (WAF), com garantia técnica de 60 (sessenta) meses”.

Contratada:

CNPJ:

Representante da Contratada:

CPF:

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

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

IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)

Nome: CPF: _____

Função/Cargo: _____

Assinatura: _____

Nome: CPF: _____

Função/Cargo: _____

Assinatura: _____

Local, UF, de de .