TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

1.1. Definição do Objeto: Registro de preços para eventual contratação de licenciamento e expansão da Solução de Segurança em Tecnologia da Informação, conforme condições e exigências estabelecidas neste instrumento.

1.2. Justificativa para a contratação:

1.2.1. O Tribunal de Justiça do Estado do Amazonas (TJAM) utiliza atualmente a solução F5 BIG-IP i5800 Best Bundle com IP Intelligence, para garantir a segurança, a alta disponibilidade e o desempenho das suas aplicações críticas, incluindo sistemas judiciais, administrativos e de serviços ao cidadão. Esta solução é fundamental para o gerenciamento avançado de tráfego, balanceamento de carga, proteção contra-ataques cibernéticos e mitigação de ameaças como DDoS e vulnerabilidades em aplicações web.

1.2.1.1. A renovação da garantia do licenciamento da solução F5 BIG-IP i5800 Best Bundle e do IP Intelligence é absolutamente essencial para assegurar a continuidade da proteção avançada das aplicações críticas do TJAM, a segurança da informação institucional e a alta disponibilidade dos serviços judiciais e administrativos prestados à sociedade. A interrupção do licenciamento comprometeria diretamente a capacidade do Tribunal de assegurar a proteção de seu ambiente tecnológico, expondo os sistemas institucionais a riscos significativos que podem afetar a integridade, a disponibilidade e a confidencialidade dos dados judiciais.

1.2.2. Demais justificativas para a contratação encontram-se pormenorizadas em tópico específico do Estudo Técnico Preliminar, anexo deste Termo de Referência.

1.3. Especificação técnica do Objeto e Quantitativo:

GRUPO	CATSER	ITEM	ESPECIFICAÇÕES	UND	QUANTIDADE MÍNIMA POR CONTRATAÇÃO	QUANTIDADE TOTAL
01	**Renovação e atualização da Solução F5 BIG-IP i5800 Best Bundle com IP Intelligence**					
	27502	1	Renovação da garantia F5 BIG-IP i5800 Best Bundle (com IP Intelligence) suporte Premium 24x7 pelo período de 06 (seis) meses.	Conjunto	01	01
	27502	2	Atualização/substituição do appliance da solução i5800 para a linha r5800 pelo período de 36 meses	Unidade	02	02
	27502	3	Licenciamento Best Bundle (com IP Intelligence) e suporte Premium 24x7 pelo período de 36 (trinta e seis) meses	Unidade	02	02
02	**Expansão módulos Distributed Cloud e Nginx**					
	27502	4	Licença Base – Distributed Cloud Base Package pelo período de 36 (trinta e seis) meses	Unidade	01	01
	27502	5	Licença F5 NGINX ONE por instância com suporte Premium 24x7 pelo período de 36 (trinta e seis) meses	Unidade	01	01
	27502	6	Licença F5 NGINX ONE por node com suporte Premium 24x7 pelo período de 36 (trinta e seis) meses	Unidade	01	04
03	**Serviços de Implantação**					
	27502	7	Serviço de migração e atualização linha “i” 5800 para “r”5800	Unidade	01	01
	27502	8	Serviço de implantação da solução Base Package (item 04)	Unidade	01	01
	27502	9	Serviço de implantação da solução NGINX ONE por node - (item 05 e/ou 06)	Unidade	01	01
	27014	10	Serviços de Consultoria e/ou Suporte Técnico (banco de horas)	Horas	100	500
VALOR TOTAL ESTIMADO DO SRP						

1.3.1. Em virtude do que foi exposto no Estudo Técnico Preliminar, a solução a ser adotada deve seguir o padrão atualmente utilizado no Tribunal de Justiça do Estado do Amazonas (TJAM), baseado na plataforma F5 BIG-IP i5800 Best Bundle, que atua como solução de segurança de aplicações, balanceamento de carga, gestão segura de acessos e proteção contra ataques cibernéticos.

1.3.2. Para manter a continuidade operacional dos serviços judiciais e administrativos, é necessária a renovação do licenciamento do ambiente atual, a substituição do hardware pela nova linha de equipamento sugerida pelo fabricante, bem como a expansão de seus componentes de software e serviços com a inclusão dos módulos F5 Distributed Cloud e F5 NGINX.

1.3.2.1. A solução escolhida deve abranger os itens descritos e elencados no quadro abaixo:

1.3.2.1.1. Grupo 1 - Renovação do licenciamento do cluster composto por dois appliances físicos do tipo F5 BIG-IP i5800 Best Bundle com IP Intelligence, com base em dados operacionais e técnicos. A renovação do contrato garantirá o suporte e as atualizações contínuas, mantendo a alta disponibilidade e a segurança das aplicações estendido pelo período mínimo de 6 (seis) meses após a data do vencimento contratual, período máximo em que a atualização/substituição do hardware deverá ser realizada e entregue a comprovação do suporte e licenciamento da linha “r” pelo período total de 36 (trinta e seis) meses;

1.3.2.1.2. Grupo 2 - Licenciamento dos módulos opcionais de expansão para o Distributed Cloud e NGINX One;

1.3.2.1.3. Grupo 3 - Refere-se aos serviços de suporte técnico especializado e/ou consultoria;

1.3.3. **Licenciamento F5 BIG-IP Best Bundle com IP Intelligence (Grupo 01)**

1.3.3.1 F5 BIG-IP i5800 Best Bundle com IP Intelligence permite reunir um conjunto de módulos avançados em uma plataforma única e integrada, voltada para garantir a otimização inteligente do tráfego, a segurança robusta das aplicações e a proteção contínua da infraestrutura de rede do Tribunal de Justiça do Estado do Amazonas (TJAM). Essa solução proporciona alta disponibilidade, desempenho aprimorado, proteção contra ameaças cibernéticas e controle refinado de acesso, atendendo a todas as necessidades de segurança e desempenho exigidas pelo ambiente crítico do Tribunal.

1.3.3.2 A seguir, descrevem-se os principais componentes da solução, com ênfase nos recursos disponibilizados por cada módulo:

1.3.3.2.1 Local Traffic Manager (LTM): O módulo Local Traffic Manager (LTM) permite a distribuição inteligente e eficiente do tráfego de rede entre os servidores, assegurando alta disponibilidade e otimização da performance das aplicações.

1.3.3.2.1.1 Distribuição dinâmica do tráfego entre múltiplos servidores, balanceando a carga de forma eficiente e prevenindo sobrecargas.

1.3.3.2.1.2 Otimização do desempenho das aplicações por meio da terminação de conexões SSL/TLS, liberando capacidade de processamento nos servidores de backend.

1.3.3.2.1.3 Definição de políticas de roteamento inteligentes baseadas em métricas como desempenho, carga e persistência de sessão.

1.3.3.2.1.4 Monitoramento contínuo da saúde dos servidores, com redirecionamento automático do tráfego em caso de falhas detectadas.

1.3.3.2.2 Application Security Manager (ASM): O módulo Application Security Manager (ASM) provê proteção avançada para aplicações web, assegurando a integridade e a disponibilidade dos serviços expostos à internet.

1.3.3.2.2.1 Implementação de políticas de segurança para mitigação de vulnerabilidades críticas, com ênfase nas ameaças mapeadas pelo OWASP Top 10.

1.3.3.2.2.2 Defesa automatizada contra ataques de bots e tráfego automatizado malicioso.

1.3.3.2.2.3 Mitigação de ataques de negação de serviço (DDoS) focados na camada de aplicação.

1.3.3.2.2.4 Inspeção profunda de pacotes (DPI) para análise comportamental do tráfego e detecção de anomalias.

1.3.3.2.2.5 Aprendizado automático para ajuste dinâmico das políticas de segurança, adaptando-se ao comportamento real das aplicações.

1.3.3.2.3 Global Traffic Manager (DNS): O módulo Global Traffic Manager (GTM), também denominado BIG-IP DNS, gerencia o tráfego DNS de forma global, direcionando os usuários para a melhor instância de serviço disponível.

1.3.3.2.3.1 Direcionamento dos usuários para o datacenter mais próximo ou com melhor desempenho, reduzindo a latência de acesso.

1.3.3.2.3.2 Balanceamento de carga entre múltiplos datacenters, garantindo a alta disponibilidade dos serviços.

1.3.3.2.3.3 Proteção contra ataques DDoS dirigidos aos serviços de DNS.

1.3.3.2.3.4 Otimização da distribuição do tráfego com base em critérios como proximidade geográfica, latência, carga e disponibilidade.

1.3.3.2.4 Advanced Firewall Manager (AFM): O módulo Advanced Firewall Manager (AFM) oferece proteção abrangente em nível de rede e transporte, mitigando ameaças volumétricas e ataques direcionados.

1.3.3.2.4.1 Inspeção e controle de tráfego nas camadas 3 e 4, com capacidade de firewall de alta performance.

1.3.3.2.4.2 Mitigação em tempo real de ataques volumétricos de DDoS, preservando a disponibilidade dos serviços críticos.

1.3.3.2.4.3 Definição de políticas de segurança adaptáveis e customizáveis conforme o perfil do tráfego e das ameaças.

1.3.3.2.4.4 Geração de relatórios detalhados de segurança e telemetria para apoio à auditoria e resposta a incidentes.

1.3.3.2.5 Access Policy Manager (APM): O módulo Access Policy Manager (APM) centraliza a autenticação e o controle de acesso dos usuários, proporcionando segurança reforçada e experiência de acesso simplificada.

1.3.3.2.5.1 Implementação de políticas de controle de acesso baseadas em função (RBAC), restringindo o acesso aos recursos conforme o perfil do usuário.

1.3.3.2.5.2 Integração nativa com mecanismos de autenticação multifator (MFA), aumentando a segurança dos acessos.

1.3.3.2.5.3 Integração com diretórios corporativos, como Active Directory, LDAP e RADIUS, para autenticação centralizada.

1.3.3.2.5.4 Suporte a Single Sign-On (SSO), permitindo que o usuário acesse múltiplas aplicações com uma única autenticação.

1.3.3.2.5.5 Disponibilização de acesso remoto seguro via portais web ou SSL VPN clientless, sem necessidade de VPN tradicional.

1.3.3.2.5.6 Avaliação da postura de segurança dos dispositivos antes da concessão do acesso, garantindo conformidade com as políticas internas.

1.3.3.3 Atualização (substituição) do hardware da solução i5800 para a linha r5800, mantendo o licenciamento atual Best Bundle com IP Intelligence e suporte premium pelo período de 36 meses, deverá atender a capacidade técnica mínima da solução conforme tabela comparativa de recursos:

Specifications	**i5800**	**r5800**
Intelligent Traffic Processing:	L7 requests per second: 1.8 M L4 connections per second: 800K L4 HTTP requests per second: 12M Maximum L4 concurrent connections: 40M Throughput: 60 Gbps/35 GbpsL4/L7	L7 requests per second: 3.3M L4 connections per second: 1.4M L4 HTTP requests per second: 18M Maximum L4 concurrent connections: 85M Throughput: 95 Gbps/85 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 20K TPS (ECDSA P-256) RSA: 35K TPS (2K Keys) 20 Gbps bulk encryption*	80K TPS (2K SSL TPS) 50K TPS (ECDHE-ECDSA P-256 TPS) 50K TPS (ECDHE P-256-RSA-2k TPS) 45 Gbps bulk encryption
Hardware Compression:	20 Gbps	40 Gbps
Hardware DDoS Protection:	50M SYN cookies per second	80M SYN cookies per second
TurboFlex™ Performance Profiles	Tier 3 (2x bandwidth)	Tier 3 (2x bandwidth)
Software Architecture:	64-bit TMOS	64-bit TMOS 64-bit F5OS
Virtualization (Maximum Number of vCMP® Guests):	8	8

1.3.4. Licenciamento F5 Distritbuted Cloud (Grupo 2)

1.3.4.1. Proteção de Aplicações Web e APIs

1.3.4.1.1 Implementar serviço em nuvem de proteção de ataques às aplicações web e APIs, disponíveis em qualquer infraestrutura pública ou privada, exposta para a Internet, sem limite de usuários, conexões, sessões e transações;

1.3.4.1.2 Implementar gestão automática de certificados digitais, incluindo a renovação dos certificados, devendo possuir integração com no mínimo o serviço Let's Encrypt (https://letsencrypt.org/);

1.3.4.1.3 Permitir a gestão manual de certificados através da importação de certificado digital e chave privada da CONTRATANTE, devendo esta ser armazenada em repositório seguro e protegido;

1.3.4.1.4 Suportar OCSP;

1.3.4.1.5 Permitir a configuração de múltiplos domínios (FQDN) para a mesma aplicação;

1.3.4.1.5.1 Suportar a gestão automática dos certificados de todos os domínios;

1.3.4.1.5.2 Suportar a gestão manual de certificados digitais e chaves privadas de todos os domínios;

1.3.4.1.5.3 Permitir a configuração de diferentes conjuntos (pools) de servidores de origem da aplicação (Origin Servers) com algoritmos de balanceamento para escolha do pool;

1.3.4.1.6 Permitir configurar pesos e prioridades diferentes para cada Pool de Origin Servers;

1.3.4.1.7 Permitir configurar um algoritmo de balanceamento de Origin Servers de um pool diferente do algoritmo de balanceamento de pools;

1.3.4.1.8 Permitir configurar monitores de disponibilidade de Origin Servers;

1.3.4.1.9 Permitir a configuração de diferentes pools de Origin Servers selecionados a partir de atributos da aplicação, incluindo no mínimo método HTTP, prefixos expressões regulares da URL e cabeçalhos HTTP;

1.3.4.1.9.1 Permitir definir políticas de WAF diferentes por pool;

1.3.4.1.10 Permitir inserir cabeçalho HSTS (HTTP Strict-Transport-Security);

1.3.4.1.11 Implementar TLS 1.2 e superiores, com algoritmos fortes e cifras que suportem PFS (Perfect Forward Secrecy);

1.3.4.1.12 Implementar Mutual TLS (mTLS) com a opção de enviar o certificado do cliente como cabeçalho HTTP para o Origin Server;

1.3.4.1.12.1 Permitir especificar a lista de Autoridades Certificadoras (CA) de validação do certificado;

1.3.4.1.12.2 Permitir verificar o certificado do cliente em listas de revogação (CRL);

1.3.4.1.12.3 Permitir enviar o certificado completo;

1.3.4.1.12.4 Permitir enviar atributos específicos do certificado;

1.3.4.1.13 Suportar HTTP/1.1 e HTTP/2;

1.3.4.1.14 Implementar inspeção e varredura com base em assinaturas para detecção de requisições maliciosas, incluindo, no mínimo proteções de:

1.3.4.1.14.1 Cross-Site Scripting (XSS);

1.3.4.1.14.2 Cross-Site Request Forgery (CSRF);

1.3.4.1.14.3 Directory Traversal;

1.3.4.1.14.4 Directory Climbing;

1.3.4.1.14.5 SQL injection;

1.3.4.1.14.6 Cookie Injection;

1.3.4.1.14.7 Command Injection;

1.3.4.1.14.8 Code Injection;

1.3.4.1.14.9 Web Parameter Tampering;

1.3.4.1.14.10 Cookie Tampering;

1.3.4.1.15 Implementar a configuração para identificação e mascaramento de dados sensíveis enviados pelo servidor para o cliente;

1.3.4.1.16 Implementar detecção e mitigação de violações do protocolo HTTP;

1.3.4.1.17 Implementar proteção contra exploração de vulnerabilidade (exploit);

1.3.4.1.18 Implementar proteção contra adulteração de cookies do serviço de proteção de aplicações;

1.3.4.1.19 Implementar inspeção, descoberta e proteção de requisições que utilizem GraphQL;

1.3.4.1.20 Permitir a configuração de políticas de segurança de permissão e bloqueio;

1.3.4.1.21 Permitir a criação de regras de exclusão de forma granular, considerando cookies, parâmetros, cabeçalhos e outros;

1.3.4.1.22 Permitir a configuração de regras de segurança positiva, onde será definido o que é permitido e todo o restante é rejeitado;

1.3.4.1.23 Permitir a configuração de políticas e regras que protejam as aplicações de ameaças e vulnerabilidades listadas no OWASP Top 10 e atualizações dessa lista;

1.3.4.1.24 Implementar proteções de campanhas de ataques e ameaças, informando a ação, o ator e a vulnerabilidade explorada;

1.3.4.1.25 Permitir criar diferentes políticas de segurança para inspeção e proteção por aplicação;

1.3.4.1.26 Permitir habilitar uma política de segurança sem bloqueios, ou seja, apenas para geração de alertas ou monitoramento;

1.3.4.1.27 Implementar mecanismos de ajuste automático de assinaturas para redução de falso-positivos;

1.3.4.1.28 Implementar fase de preparação de assinaturas de ataque, quando assinaturas novas e atualizadas são configuradas no modo de monitoramento por um período;

1.3.4.1.29 Permitir desabilitar inspeções para tipos de ataques específicos;

1.3.4.1.30 Permitir definir os códigos de respostas HTTP (status code) que serão aceitos vindos da aplicação original, quando os demais códigos serão bloqueados;

1.3.4.1.31 Permitir ocultar atributos e parâmetros sensíveis, tais como senhas ou outros dados sensíveis, em mensagens de log da plataforma;

1.3.4.1.32 Permitir a criação de diferentes páginas de respostas de bloqueio, fornecendo um identificador de requisição;

1.3.4.1.33 Permitir a criação de diferentes páginas de respostas por códigos de respostas HTTP (status code);

1.3.4.1.34 Implementar a identificação de usuários e clientes a partir de informações extraídas de cabeçalhos IP, HTTP, parâmetros, cookies, JWT e fingerprint do TLS;

1.3.4.1.35 Não serão aceitas soluções que classificam usuários apenas a partir do IP de origem;

1.3.4.1.36 Implementar limitação de tráfego (rate limit) por usuário;

1.3.4.1.37 Permitir a criação de regras de bloqueio com base na classificação do IP de origem e sua reputação;

1.3.4.1.37.1 Deve possuir, pelo menos, a classificação de IP para botnets, scanners, proxies anônimos, proxies ToR e origens conhecidas de ataques web;

1.3.4.1.38 Permitir a definição de taxa máxima de requisições (rate limit);

1.3.4.1.39 Permitir definir uma lista de clientes confiáveis que não serão bloqueados por regras da política de segurança;

1.3.4.1.40 Permitir definir uma lista de clientes suspeitos que devem ser bloqueados;

1.3.4.1.41 Implementar a inspeção com base no IP do cliente que iniciou a conexão e permitir utilizar o IP do cliente, o cabeçalho X-Forwarded-For por exemplo, presente no cabeçalho HTTP;

1.3.4.1.42 Permitir inserir cabeçalho HTTP na requisição e na resposta;

1.3.4.1.43 Permitir remover cabeçalhos HTTP da requisição;

1.3.4.1.44 Implementar o redirecionamento automático de HTTP para HTTPS;

1.3.4.1.45 Permitir a configuração de políticas de CORS (Cross-Origin Resource Sharing);

1.3.4.1.46 Implementar mitigação automática de DDoS em camada 7;

1.3.4.1.47 Implementar mitigação automática de ataques “Slow and low”;

1.3.4.2 Implementar defesa automática de ataques de Distributed Denial-Of-Service (DDoS), protegendo continuamente todas as aplicações publicadas através do serviço contratado em nuvem;

1.3.4.2.1 Deve mitigar ataques de forma transparente para a aplicação, absorvendo e bloqueando ataques;

1.3.4.2.2 Deve ser capaz de detectar ataques através da análise das taxas de requisição, erros, latência e throughput da aplicação;

1.3.4.2.3 Implementar proteção de ataques na camada de aplicação, incluindo os protocolos HTTP e DNS, incluindo, no mínimo, proteções de HTTP GET Flood, HTTP POST Flood, Slowloris e DNS Flood;

1.3.4.2.4 Implementar proteção de ataques volumétricos, incluindo SYN Flood, UDP Flood, TCP Flood e ICMP Flood;

1.3.4.2.5 Implementar proteção de ataques de negação de serviço através da exaustão de recursos (“Slow DDoS”), incluindo Slow POST e Slowloris;

1.3.4.2.6 Implementar proteção de ataques à pilha TCP;

1.3.4.2.7 Implementar proteção de ataques que utilizam falsificação de endereços IP de origem (IP spoofing);

1.3.4.2.8 Implementar detecção e mitigação automática de ataques em Camada 7 em larga escala;

1.3.4.2.9 Implementar proteção através de bloqueio geográfico e de, pelo menos, 100 (cem) prefixos IP;

1.3.4.2.10 Permitir criar regras de respostas personalizadas;

1.3.4.2.11 Permitir configurar o bloqueio de clientes com base no TLS fingerprint;

1.3.4.2.12 Permitir configurar o bloqueio de clientes com base na classificação e reputação do IP;

1.3.4.2.12.1 Deve possuir, pelo menos, a classificação de IP para botnets, scanners, proxies anônimos, proxies ToR e origens conhecidas por ataques web;

1.3.4.2.13 Permitir configurar o bloqueio de clientes com base no ASN do BGP;

1.3.4.2.14 Permitir configurar de mitigações específicas por aplicação;

1.3.4.2.15 Permitir configurar rate limit por aplicação;

1.3.4.2.16 Permitir configurar rate limit por usuário, onde entende-se por usuário como sendo um cliente da aplicação identificado por um IP de origem, um cookie, um cabeçalho, parâmetro da query, fingerprint TLS, geolocalização, ou combinação de alguns desses;

1.3.4.3 Implementar serviço DNS primário e secundário;

1.3.4.3.1 Implementar zona de pesquisa direta (Forward DNS Lookup Zone) e reverso (Reverse Lookup Zone);

1.3.4.3.2 Para as zonas hospedadas na solução, implementar a configuração automática de domínios e FQDN utilizados nas aplicações publicadas pela solução;

1.3.4.3.3 Possuir interface gráfica para gerenciamento de registros do DNS;

1.3.4.3.4 Implementar DNSSEC (Domain Name System Security Extensions) com gerenciamento automático de chaves;

1.3.4.3.5 Implementar proteções de ataques direcionados aos serviços de DNS;

1.3.4.3.6 Implementar proteções de ataques de DDoS;

1.3.4.3.7 Implementar a configuração de registros de DNS para funcionalidade de balanceamento de sites (Global Server Load Balancer – GSLB);

1.3.4.3.7.1 Implementar a verificação de disponibilidade dos sites através de testes HTTP e ICMP;

1.3.4.3.7.2 Implementar, pelo menos, os algoritmos de balanceamento round robin, prioridade, peso e origem;

1.3.4.3.7.3 Implementar persistência da resolução dos elementos utilizando, pelo menos, o Local DNS da requisição;

1.3.4.3.7.4 Permitir configurar topologias para respostas com base em geolocalização;

1.3.4.4 Os serviços devem ser prestados através de infraestrutura em nuvem do próprio fabricante da solução de forma não intrusiva, ou seja, sem a necessidade de instalação de equipamentos ou softwares nas dependências da CONTRATANTE;

1.3.4.4.1 O serviço em nuvem deverá ser oferecido em ponto(s) de presença em território nacional;

1.3.4.4.2 As atividades de administração, gerenciamento, operação e monitoramento dos serviços deverão ser através de console web única, gráfica e central do fabricante da solução, via HTTPS com algoritmos de criptografia modernos e seguros, compatível com navegadores padrões, não sendo aceitas soluções que dependam de plugins, add-ons ou aplicação exclusiva instaladas nas estações de trabalho;

1.3.4.4.3 A console deve possuir controles de segurança, incluindo, mas não se limitando a, restrição de acesso administrativo por meio de um login seguro com autenticação de dois fatores de modo a prevenir que os serviços não sejam utilizados por terceiros não autorizados;

1.3.4.4.4 Permitir a criação de divisões administrativas de recursos através da criação de segmentos, partições, namespaces ou estrutura semelhante para agrupamento de recursos de diferentes propósitos, áreas ou finalidades da CONTRATANTE, tais como “Produção”, “Homologação” e “Desenvolvimento”, unidade de negócio, departamento, entre outros;

1.3.4.4.5 Permitir a criação de usuários com acesso à console;

1.3.4.4.6 Permitir a utilização de provedores de identidade para autenticação e autorização de usuários sem a necessidade de importar ou sincronizar com bases externas de usuários e senhas;

1.3.4.4.7 Implementar Single Sign-On (SSO) compatível com OpenID Connect (OIDC), tais como Okta, Microsoft, Google e outros;

1.3.4.4.8 Permitir a configuração de Segundo Fator de Autenticação;

1.3.4.4.9 Permitir a criação de credenciais para acesso via API com data de expiração ou prazo de validade;

1.3.4.4.10 Permitir definir políticas de senhas, incluindo tipo de caracteres, tamanho mínimo, validade e tentativas malsucedidas;

1.3.4.4.11 Permitir a criação de grupos de usuários e associar usuários aos grupos;

1.3.4.4.12 Deve permitir a criação de perfis de acesso com diferentes níveis de acesso aos recursos da solução;

1.3.4.4.12.1 Dispor de diferentes perfis predefinidos com diferentes níveis de acesso para diferentes recursos da solução, incluindo acesso restrito, somente leitura, e leitura e escrita;

1.3.4.4.12.2 Permitir associar perfis de acesso a usuários por divisão administrativa;

1.3.4.4.12.3 Permitir associar perfis de acesso a grupos de usuários por divisão administrativa;

1.3.4.4.13 Implementar API REST autenticada através de tokens ou certificados para configuração de recursos, com documentação pública mantida pelo fornecedor do serviço;

1.3.4.4.14 Deve ser compatível com mTLS;

1.3.4.4.15 Dispor de um cliente de linha de comando (CLI) que implemente a API REST compatível com, pelo menos, Linux e Mac OS;

1.3.4.4.16 Possuir implementações específicas para ferramentas de automação no formato de provedores e módulos para Terraform ou coleções para Ansible;

1.3.4.4.17 Permitir a exportação de eventos para sistemas externos, incluindo logs da solução e de requisições, segurança, e auditoria das aplicações;

1.3.4.4.18 Permitir a exportação para, pelo menos, os seguintes sistemas: Kafka, Splunk, Datadog, Azure, Amazon, QRadar e servidores HTTPS genéricos;

1.3.4.4.19 Permitir a configuração, pelo menos, 02 (dois) destinos para envio de eventos;

1.3.4.4.20 Possuir painéis online para visualização de eventos e estatísticas, incluindo, no mínimo:

1.3.4.4.20.1 Saúde geral da aplicação;

1.3.4.4.20.2 Latência fim a fim;

1.3.4.4.20.3 Estatísticas de TLS;

1.3.4.4.20.4 Eventos com origem, destino, ataque e ação;

1.3.4.4.20.5 Taxas de requisições, status code e métodos;

1.3.4.4.20.6 Latência e throughput da aplicação;

1.3.4.4.20.7 Total de requisições ao longo do tempo;

1.3.4.4.20.8 Lista de aplicações e requisições, ataques e bloqueios;

1.3.4.4.20.9 Tipos de eventos;

1.3.4.4.20.10 Ataques, origens e alvos mais comuns;

1.3.4.4.20.11 Assinaturas e violações mais comuns;

1.3.4.4.20.12 Sumário de segurança;

1.3.4.4.20.13 Classificação de bots das requisições;

1.3.4.4.20.14 Volume de requisições de bots e humanos;

1.3.4.4.20.15 Fluxos da aplicação mais atacados por bots;

1.3.4.4.20.16 Lista de bots maliciosos por origem IP e tipo;

1.3.4.4.20.17 Informações de origem geográfica, dispositivos e plataformas relacionadas a bots;

1.3.4.4.20.18 Eventos de DDoS ao longo do tempo;

1.3.4.4.20.19 Taxa de requisições de ataques de DDoS;

1.3.4.4.20.20 Throughput do DDoS;

1.3.4.4.20.21 Mapa geográfico indicando a origem do DDoS;

1.3.4.4.20.22 Origens, regiões e ASN (Autonomous System Number) mais comuns relacionadas ao ataque de DDoS;

1.3.4.4.20.23 Mapa geográfico das requisições de DNS por zona;

1.3.4.4.20.24 Gráfico de volume de requisições ao longo do tempo de DNS;

1.3.4.4.20.25 Lista de nomes de DNS mais solicitados;

1.3.4.4.20.26 Lista de tipos de requisições de DNS mais solicitadas e gráfico ao longo do tempo;

1.3.4.4.20.27 Gráfico de volume por tipo de resposta de DNS ao longo do tempo;

1.3.4.4.21 Possuir relatório de incidentes de segurança para investigação de ataques com agrupamento automático de eventos em incidentes;

1.3.4.4.22 Permitir a configuração de agendamento de relatórios (diários, semanais ou mensais) e enviar os resultados por e-mail para usuários específico;

1.3.4.4.23 Recursos Disponíveis por Unidade do Serviço de Base Package

1.3.4.4.23.1 Permite a configuração de 01 (um) Load Balancer, sem limite de Origin Servers, com franquia de 5 (cinco) TB por mês de volume de transferência de dados sem considerar tráfego de ataques;

1.3.4.4.23.2 Entende-se por aplicação como a configuração de um FQDN ou domínio que deve ser protegido por uma política de segurança, acessível através da infraestrutura em nuvem por um IP ou CNAME, independente da quantidade de paths ou URL deste FQDN;

1.3.4.4.23.3 Capacidade de limitar taxas de requisições válidas (rate limit) de usuários identificados de, no mínimo, 300.000 (trezentas mil) requisições/dia entre todas as aplicações;

1.3.4.4.23.4 Capacidade de descobrir as API em, no mínimo, 05 (cinco) aplicações, independente da quantidade de requisições/dia;

1.3.4.4.23.5 Capacidade de proteger as APIs de, no mínimo, 150.000 (cento e cinquenta mil) requisições/dia válidas entre todas as aplicações;

1.3.4.4.23.6 Capacidade de proteção de bots de, no mínimo, 500.000 (quinhentas mil) transações/dia entre todas as aplicações;

1.3.4.4.23.7 Capacidade de realizar testes de vulnerabilidades para 03 (três) aplicações/mês;

1.3.4.4.23.8 Capacidade de realizar varreduras em domínios para 01 (um) domínio/mês;

1.3.4.4.23.9 Capacidade de mitigar DDoS independente do volume de tráfego, sem custo adicional;

1.3.4.4.23.10 Serviço de DNS autoritativo primário e secundário para, no mínimo, 150 (cento e cinquenta) zonas, sem limite de resoluções e resposta de DNS;

1.3.4.4.23.11 Serviço de balanceamento de DNS para, pelo menos 30 (trinta) endereços IP;

1.3.4.4.23.12 Garantir via console o acesso, busca e consulta de eventos por, no mínimo:

1.3.4.4.23.12.1 30 (trinta) dias para métricas de desempenho e eventos de auditoria;

1.3.4.4.23.12.2 07 (sete) dias para eventos de requisições e segurança;

1.3.4.4.23.12.3 Para eventos mais antigos, a solução deve garantir o armazenamento de, pelo menos, 50 (cinquenta) GB de mensagens ou manter os eventos por até 30 dias.

1.3.5. Licenciamento F5 NGINX (Grupo 2)

1.3.5.1. Características técnicas

1.3.5.1.1. Deve ser compatível com, pelo menos, os seguintes ambientes:

1.3.5.1.1.1. Bare metal

1.3.5.1.1.2. Container

1.3.5.1.1.3. Public cloud: AWS, Google Cloud Platform, Microsoft Azure

1.3.5.1.1.4. Virtual machine

1.3.5.1.2. Deve ser suportado, em pelo menos, nos seguintes sistemas operacionais:

1.3.5.1.2.1. Alpine Linux

1.3.5.1.2.1.1. 3.12 (x86_64, aarch64)

1.3.5.1.2.1.2. 3.13 (x86_64, aarch64)

1.3.5.1.2.1.3. 3.14 (x86_64, aarch64)

1.3.5.1.2.1.4. 3.15 (x86_64, aarch64)

1.3.5.1.2.2. Amazon Linux 2

1.3.5.1.2.2.1. LTS (x86_64, aarch64)

1.3.5.1.2.3. CentOS

1.3.5.1.2.3.1. 7.4+ (x86_64, aarch64, ppc64le)

1.3.5.1.2.3.2. 8.1+ (x86_64, aarch64, s390x)

1.3.5.1.2.4. Debian

1.3.5.1.2.4.1. 10 (x86_64, aarch64)

1.3.5.1.2.4.2. 11 (x86_64, aarch64)

1.3.5.1.2.5. FreeBSD

1.3.5.1.2.5.1. 12.1+ (amd64)

1.3.5.1.2.5.2. 13 (amd64)

1.3.5.1.2.6. Oracle Linux

1.3.5.1.2.6.1. 7.4+ (x86_64)

1.3.5.1.2.6.2. 8.1+ (x86_64, aarch64)

1.3.5.1.2.7. Red Hat Enterprise Linux (RHEL)

1.3.5.1.2.7.1. 7.4+ (x86_64, aarch64, ppc64le)

1.3.5.1.2.7.2. 8.1+ (x86_64, aarch64, s390x)

1.3.5.1.2.8. SUSE Linux Enterprise Server (SLES)

1.3.5.1.2.8.1. 12 SP5 (x86_64)

1.3.5.1.2.8.2. 15 SP2 (x86_64)

1.3.5.1.2.9. Ubuntu

1.3.5.1.2.9.1. 18.04 LTS (x86_64, aarch64)

1.3.5.1.2.9.2. 20.04 LTS (x86_64, aarch64, s390x)

1.3.5.1.3. Deve possuir ao menos um processo master e um processo worker

1.3.5.1.3.1. O processo master deve ser responsável pela leitura dos arquivos de configuração

1.3.5.1.3.2. O processo worker deve ser responsável pelo processamento das requisições

1.3.5.1.3.3. Deve ser possível configurar manualmente o número de processos worker

1.3.5.1.3.4. Deve ser possível ajustar automaticamente o número de processos worker com base na quantidade de CPU disponível

1.3.5.1.4. Quando a solução realizar cache devem existir processos específicos de cache loader e cache manager

1.3.5.1.5. Deve permitir aplicar as alterações na configuração sem interromper o processamento das requisições

1.3.5.1.6. Deve permitir a reconfiguração dinâmica do balanceamento dos servidores sem a necessidade de realizar reload da configuração

1.3.5.1.7. Deve possuir a capacidade de operar em alta disponibilidade nos modos ativo-ativo e ativo-standby

1.3.5.1.8. Deve suportar uso em alta disponibilidade com, pelo menos as seguintes funções:

1.3.5.1.8.1. Session caching: as sessões são compartilhadas entre os nodes

1.3.5.1.8.2. Resource limiting: cada node avalia os recursos locais e notifica os outros

1.3.5.1.8.3. Dynamic configuration: mudanças dinâmicas na configuração são compartilhadas entre os nodes

1.3.5.1.9. Deve realizar, pelo menos, os seguintes métodos de balanceamento do tráfego HTTP:

1.3.5.1.9.1. Round robin

1.3.5.1.9.2. Least connections

1.3.5.1.9.3. IP Hash

1.3.5.1.9.4. Generic Hash

1.3.5.1.9.5. Least time

1.3.5.1.10. Deve realizar, pelo menos, os seguintes métodos de balanceamento do tráfego TCP e UDP:

1.3.5.1.10.1. Round robin

1.3.5.1.10.2. Least connections

1.3.5.1.10.3. Hash

1.3.5.1.10.4. Least time

1.3.5.1.11. Deve ser capaz de configurar o tempo no qual as conexões para um servidor crescem gradativamente

1.3.5.1.12. Deve realizar o processamento de tráfego HTTP

1.3.5.1.13. Deve permitir a inclusão de dados na resposta dos servidores/aplicações

1.3.5.1.14. Deve ser capaz de realizar o processamento de requisições que terminem em "/"

1.3.5.1.15. Deve ser capaz de manipular a resposta do servidor e especificar o content-type

1.3.5.1.16. Deve ser capaz de gerar um gif com apenas um pixel

1.3.5.1.17. Deve ser capaz de retirar a compressão da resposta dos servidores para enviar aos clientes que não possuem suporte a GZIP

1.3.5.1.18. Deve ser capaz de realizar a compressão da resposta do servidor antes de enviar aos clientes

1.3.5.1.19. Deve ser capaz de adicionar campos na resposta do servidor antes de enviar para os clientes

1.3.5.1.20. Deve ser capaz de definir arquivos que serão utilizados no index

1.3.5.1.21. Deve ser capaz de tornar aleatória a escolha do arquivo de index

1.3.5.1.22. Deve ser capaz de alterar IP e porta do cliente para valores que estiverem no cabeçalho

1.3.5.1.23. Deve ser capaz de realizar filtragem de comandos nas respostas

1.3.5.1.24. Deve ser capaz de definição de cookies para identificação dos clientes

1.3.5.1.25. Deve ser capaz de gerenciamento de arquivos para facilitar a atualização dos websites utilizando WebDAV

1.3.5.1.26. Deve possuir suporte a Brotli como algoritmo para compressão de dados

1.3.5.1.27. Deve ser capaz de realizar a identificação da localização do cliente pelo IP, contendo: região, estado, cidade, ISP

1.3.5.1.28. Deve possuir suporte a Lua para manipulação de requisições MySQL, PostgreSQL, Memcached, Redis, e upstream HTTP web services

1.3.5.1.29. A solução deve, quando habilitado, permitir a proteção das aplicações através de WAF

1.3.5.1.30. A solução deve ter suporte ao uso de framework para rastreamento do cliente, compatível com Zipkin, Jaeger e Datadog

1.3.5.1.31. A solução deve ter suporte ao controle de acesso baseado em endereço IP (Access Control List - ACL)

1.3.5.1.32. A solução deve implementar autenticação HTTP Basic

1.3.5.1.33. A solução deve realizar validação de JSON Web Tokens

1.3.5.1.34. A solução deve realizar autorização de clientes através de requisições a um autenticador externo

1.3.5.1.35. A solução deve realizar controle de acesso através do campo Referer contido no cabeçalho HTTP

1.3.5.1.36. A solução deve realizar verificação de autenticidade através do tempo de expiração do link

1.3.5.1.37. A solução deve realizar a criação de variáveis baseado no valor do User-Agent contido no cabeçalho HTTP dos clientes

1.3.5.1.38. A solução deve dividir as requisições em sub-requisições e cada uma poderá ser respondida com cache

1.3.5.1.39. A solução deve permitir a criação de variáveis baseadas em outras variáveis

1.3.5.1.40. A solução deve permitir a alteração da URI solicitada ou realizar o redirect

1.3.5.1.41. A solução deve realizar segregação de tráfego baseado em variáveis (Teste A/B)

1.3.5.1.42. A solução deve realizar alteração de textos na resposta aos clientes

1.3.5.1.43. A solução deve logar transações HTTP local ou remotamente

1.3.5.1.44. A solução deve realizar a agregação de log das transações HTTP por sessão

1.3.5.1.45. Deve realizar proxy para, pelo menos, as seguintes tecnologias:

1.3.5.1.45.1. F4F: Stream HDS (Adobe HTTP Dynamic Streaming; filename extensions .f4f, .f4m, .f4x)

1.3.5.1.45.2. FLV: realizar Stream FLV (Flash Video; filename extension .flv)

1.3.5.1.45.3. HLS: realizar Stream HLS (Apple HTTP Live Streaming; filename extensions .m3u8, .ts) dinamicamente gerado de MP4 ou MOV (extensões .m4a, .m4v, .mov, .mp4, .qt)

1.3.5.1.45.4. MP4: realizar Stream MP4 (extensões .m4a, .m4v, .mp4)

1.3.5.1.45.5. FastCGI: realizar Proxy e cache das requisições para FastCGI server

1.3.5.1.45.6. gRPC: realizar Proxy das requisições para gRPC server

1.3.5.1.45.7. Memcached: realizar Proxy das requisições para memcached server

1.3.5.1.45.8. Mirror: enviar cópias das requisições para um ou mais servidores

1.3.5.1.45.9. Proxy: realizar Proxy e cache das requisições para HTTP server

1.3.5.1.45.10. SCGI: realizar Proxy e cache das requisições para SCGI server

1.3.5.1.45.11. Upstream: realizar Proxy e cache das requisições para servidores que estão sendo balanceados

1.3.5.1.45.12. Uwsgi: realizar Proxy e cache das requisições para uwsgi server

1.3.5.1.46. Deve suportar a monitoração dos servidores que estão sendo balanceados através, pelo menos, dos seguintes parâmetros:

1.3.5.1.46.1. Intervalo entre monitoração

1.3.5.1.46.2. Variação do tempo entre cada monitoração

1.3.5.1.46.3. Falhas consecutivas (quantidade de falhas para considerar o servidor "fora do ar")

1.3.5.1.46.4. Acertos consecutivos (quantidade de acertos para considerar o servidor “no ar”)

1.3.5.1.41.3.3. URI

1.3.5.1.41.3.4. Porta

1.3.5.1.41.3.5. gRPC

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

1.3.5.1.47.1. Por cookie: inserção de um novo cookie na sessão

1.3.5.1.47.2. Por cookie: utilização do valor do cookie da aplicação

1.3.5.1.48. Deve realizar controle de tráfego HTTP através de, pelo menos, os seguintes parâmetros:

1.3.5.1.48.1. Limitação de quantidade de conexões

1.3.5.1.48.2. Limitação de quantidade de requisições

1.3.5.1.48.3. Limitação de quantidade de respostas

1.3.5.1.49. Deve possuir suporte a HTTP/2

1.3.5.1.50. Deve suportar, pelo menos, os seguintes padrões de SSL/TLS:

1.3.5.1.50.1. SSLv2

1.3.5.1.50.2. SSLv3

1.3.5.1.50.3. TLSv1

1.3.5.1.50.4. TLSv1.1

1.3.5.1.50.5. TLSv1.2

1.3.5.1.50.6. TLSv1.3

1.3.5.1.51. Deve suportar a realização de proxy para protocolos de correio eletrônico:

1.3.5.1.51.1. IMAP

1.3.5.1.51.2. POP3

1.3.5.1.51.3. SMTP

1.3.5.1.52. Deve possibilitar a configuração através de REST API

1.3.5.1.53. Deve realizar o controle de acesso utilizando autenticação JWT

1.3.5.1.54. Deve realizar o controle de acesso utilizando a geolocalização do IP de origem

1.3.5.2. Ingress Controller

1.3.5.2.1 Deve ser compatível com, pelo menos, os seguintes ambientes Kubernetes:

1.3.5.2.1.1 Kubernetes 1.24 – 1.19

1.3.5.2.1.2 NIC Helm Chart 0.14.0

1.3.5.2.1.2 NIC Operator 1.1.0

1.3.5.2.2 Deve estar disponível como Docker image em pelo menos:

1.3.5.2.2.1 Alpine 3.16

1.3.5.2.2.2 Debian bullseye-slim

1.3.5.2.2.3 Debian buster-slim

1.3.5.2.2.4 RedHat ubi8

1.3.5.2.3 Deve ser compatível com Kubernetes Ingress API v1

1.3.5.2.4 Deve realizar circuit breaking

1.3.5.2.5 Deve realizar distribuição blue-green

1.3.5.2.6 Deve realizar canary testing

1.3.5.2.7 Deve realizar A/B testing

1.3.5.2.8 Deve realizar routing

1.3.5.2.9 Deve realizar header manipulation

1.3.5.2.10 Deve realizar autenticação mTLS

1.3.5.2.11 Deve realizar WAF

1.3.5.2.12 Deve suportar WebSocket

1.3.5.2.13 Deve realizar reescrita de URL

1.3.5.2.14 Deve suportar HTTP/2

1.3.5.2.15 Deve ser compatível com Helm Charts

1.3.5.2.16 Deve realizar persistência de sessão

1.3.5.2.17 Deve realizar monitoração em tempo real

1.3.5.2.18 Deve realizar a monitoração out-of-band da aplicação, também conhecida como synthetic transaction

1.3.5.2.19 Deve ser capaz de configurar o tempo no qual as conexões para um servidor crescem gradativamente

1.3.5.2.20 Deve possuir controle de acesso role-based access control (RBAC), onde cada time poderá gerenciar suas próprias aplicações sem ter acesso às outras aplicações

1.3.5.2.21 Deve disponibilizar estatísticas em tempo real do tráfego

1.3.5.2.22 Deve possuir integração nativa com Grafana e Prometheus

1.3.5.2.23 Deve exportar, pelo menos, as seguintes métricas para o Prometheus:

1.3.5.2.23.1 Accepted client connections

1.3.5.2.23.2 Active client connections

1.3.5.2.23.3 Dropped client connections

1.3.5.2.23.4 Total http requests

1.3.5.2.23.5 Current http requests

1.3.5.2.23.6 Successful SSL handshakes

1.3.5.2.23.7 Failed SSL handshakes

1.3.5.2.23.8 Session reusing during SSL handshakes

1.3.5.2.23.9 Client connections that are currently being processed

1.3.5.2.23.10 Total Connections

1.3.5.2.23.11 Total Sessions Completed

1.3.5.2.23.12 Connections completed without creating a session

1.3.5.2.23.13 Bytes received from clients

1.3.5.2.23.14 Bytes sent to clients

1.3.5.2.24 Deve realizar a reconfiguração dinâmica dos serviços expostos, assim quando o número de pods for alterado não será necessário realizar o reload da configuração

1.3.6. Serviços de Implantação e Configuração (Grupo 03)

1.3.6.1 Serviços de atualização e migração para o novo appliance

1.3.6.1.1 Os novos appliances deverão ser entregues na sede da contratante e será de responsabilidade do Orgão:

1.3.6.1.1.1 Instalar fisicamente o apliance no rack;

1.3.6.1.1.2 Conectar cabos de rede (dados e HA) e de gerenciamento;

1.3.6.1.1.3 Todas estas atividades poderão ser feitas com o acompanhamento remoto da contratada;

1.3.6.1.2 Deverá ser realizado um inventário e levantamento do ambiente atual:

1.3.6.1.2.1 Versão TMOS e hotfixes instalados;

1.3.6.1.2.2 Módulos licenciados e configurados (LTM, ASM/Advanced WAF, DNS/GTM, APM, etc.);

1.3.6.1.2.3 Perfis, políticas e objetos compartilhados;

1.3.6.1.2.4 Licenciamento atual (chave de ativação) e suporte;

1.3.6.1.2.5 Recursos utilizados: CPU, memória, throughput, conexões ativas;

1.3.6.1.2.6 Topologia física e lógica (interfaces, VLANs, trunks, HA, VRRP/failover groups);

1.3.6.1.2.7 Lista de VIPs, pools, nodes e regras iRules/iApps/iLX;

1.3.6.1.2.8 Configurações de certificados, chaves, perfis SSL.

1.3.6.1.3 Validação de compatibilidade no momento da migração;

1.3.6.1.3.1 Confirmar versão do TMOS suportada pelo r5800 (ideal manter mesma versão no momento da migração para evitar reconfigurações);

1.3.6.1.3.2 Checar possíveis ajustes necessários devido a diferenças de hardware (drivers, interfaces, módulos);

1.3.6.1.4 Elaborar plano de migração contendo:

1.3.6.1.4.1 Procedimento para rollback em cado de falha;

1.3.6.1.4.2 Testes de conectividade;

1.3.6.1.5 Migração das configurações:

1.3.6.1.5.1 Procedimento de migração do i5800 (gerar backup, exportar arquivos, entre outros);

1.3.6.1.5.2 Procedimentos para o r5800 (ajustar os parâmetros de rede necessários, aplicar nova licença, validar os módulos e recursos ativados;

1.3.6.1.5.3 Exportat e importar objetos e políticas de acordo com os procedimentos listados no guide da F5 Networks;

1.3.6.1.6 Testes e Validações

1.3.6.1.6.1 Testes de conectividade Testar todas as VIPs e serviços configurados (LTM, WAF, DNS, APM);

1.3.6.1.6.2 Validar health monitors e status de pools/nodes;

1.3.6.1.6.3 Testar persistência, iRules, compressão, SSL offload;

1.3.6.1.6.4 Validar HA (failover manual entre appliances se em par);

1.3.6.1.6.5 Medir performance básica (latência, throughput);

1.3.6.1.7 Ativação em produção

1.3.6.1.7.1 Programar janela de mudança;

1.3.6.1.7.2 Trocar cabos/tráfego para o novo r5800;

1.3.6.1.7.3 Monitorar métricas e logs;

1.3.6.1.8 Pós-Migração

1.3.6.1.8.1 Registrar serial e ativar suporte no myF5;

1.3.6.1.8.2 Atualizar documentação de topologia e configurações;

1.3.6.1.8.3 Desativar o i5800 conforme planejamento realizado;

1.3.7. Serviços de implantação e Configuração para o Base Package:

1.3.7.1. HTTP Load Balancers

1.3.7.1.1 Será configurado um HTTP Load Balancer contendo até 15 FQDNs para atender às aplicações do ambiente, com as seguintes características, conforme necessário:

1.3.7.1.1.1 Domains and LB Type.

1.3.7.1.1.2 Custom TLS Certificate.

1.3.7.1.1.3 Routes.

1.3.7.2 Origin Pools

1.3.7.2.1 Será criado um Pool com um ou mais servidores reais que atendem a cada aplicação associada a um HTTP Load Balancer. As informações necessárias (IP/DNS, Porta) deverão ser fornecidas previamente à instalação.

1.3.7.2.2 Configuração de Health Check

1.3.7.3 Web Application Firewall (WAF)

1.3.7.3.1 Configuração da Política de Segurança

1.3.7.3.1.1 Será criada uma política de WAF para cada HTTP Load Balancer, com as seguintes características:

1.3.7.3.1.1.1 Attack Signatures: All Attack Types, High and Medium Signatures.

1.3.7.3.1.1.2 Automatic Attack Signatures Tuning.

1.3.7.3.1.1.3 Threat Campaigns.

1.3.7.3.1.1.4 Violations.

1.3.7.3.1.1.5 Signature-Based Bot Protection.

1.3.7.4.2 Operação

1.3.7.4.2.1 As políticas de segurança serão criadas com aprendizado automático e configuradas inicialmente em modo transparente (sem bloqueio). A contratante deverá acompanhar a evolução da ferramenta e, após a fase de aprendizado, mudar o estado para bloqueio, efetivando a política e minimizando possíveis impactos.

1.3.7.5 DoS Protection

1.3.7.5.1 Será configurado o DoS Protection para cada HTTP Load Balancer, com as seguintes características:

1.3.7.5.1.1 L7 DDoS Auto Mitigation;

1.3.7.5.1.2 Slow DDoS Mitigation.

1.3.7.6 Common Security Controls

1.3.7.6.1 Service Policies

1.3.7. 6.1.1 Serão configuradas até 5 service policies, que poderão ser replicadas para mais de um HTTP Load Balancer.

1.3.7.6.2 IP Reputation

1.3.7.6.2.1 Será configurado o IP Reputation, abrangendo um HTTP Load Balancer.

1.3.7.6.3 Threat Mesh

1.3.7.6.3.1 Será configurado o Threat Mesh, abrangendo um HTTP Load Balancer.

1.3.7.6.4 Global Log Receiver

1.3.7.6.4.1 Será criado um Global Log Receiver com o objetivo de enviar os logs para um sistema externo de coleta, incluindo logs relacionados a: logs de Requisição, eventos de segurança e logs de auditoria.

1.3.7.7 Serviços de Configuração para API Protection

1.3.7.7.1 Será configurado o API Protection, abrangendo um HTTP Load Balancer, com as seguintes características:

1.3.7.7.1.1 A configuração do API Validation será realizada no modo 'report', com base no API Inventory importado, permitindo a solicitação e gerando um evento de segurança da API. A contratante, após validar o arquivo OpenAPI Specification gerado, poderá alterar a configuração para o modo 'block'.

1.3.7.7.1.2 Será configurada a regra de proteção de API para até 5 API endpoints.

1.3.7.7.1.3 Será configurado o rate limiting de API para até 10 API endpoints.

1.3.7.8 Malicious Users

1.3.7.8.1 Será configurado o Malicious User para um HTTP Load Balancer, com os seguintes critérios:

1.3.7.8.1.1 Configuração para identificação de usuários;

1.3.7.8.1.2 Configuração para detecção de usuários maliciosos, com a exibição de informações sobre o nível de ameaça com base nas atividades do usuário.

1.3.7.9 Serviços de Configuração para o Bot Defense

1.3.7.9.1 Será configurada a proteção contra bots para uma aplicação/FQDN específico, com os seguintes critérios:

1.3.7.9.1.1 A configuração inicial será realizada com até 5 endpoints, em modo learning/transparente. A contratante será responsável por alterar a configuração para o modo block, caso deseje.

1.3.7.10 Serviços de Configuração para o Web App Scan

1.3.7.10.1 Será realizada uma varredura automatizada do ambiente, por domínio, com o objetivo de identificar os serviços expostos e detectar possíveis problemas.

1.3.7.10.2 Será realizada uma segunda varredura em modo de Scan para até um serviço/aplicação, identificada pelo módulo de Recon, com o objetivo de analisar vulnerabilidades.

1.3.8. Serviços de Configuração para o NGINX ONE por node

1.3.8.1 Será realizada a implementação do NGINX Ingress Controller com Integração Automatizada via F5 BIG-IP, CIS, IngressLink e IPAM para Ambientes Kubernetes.

1.3.8.2 Descrição do Serviço

1.3.8.2.1 A implementação completa e otimizada do NGINX Ingress Controller em ambientes Kubernetes em 01 Cluster, será integrado de forma automatizada ao F5 BIG-IP por meio dos recursos avançados do F5 Container Ingress Services (CIS), IngressLink e IPAM Controller.

1.3.8.2.2 Este serviço visará modernizar a camada de entrada (ingress) das aplicações, proporcionando automação, segurança, visibilidade e alta disponibilidade no roteamento de tráfego externo para serviços em containers.

1.3.9. Serviços de Consultoria e Suporte Técnico

1.3.9.1 Serviços que não se aplicam a este grupo e já estão cobertos pela garantia do fabricante e que serão destacados no item 6.5:

1.3.9.1.1 Serviços que visam garantir a resolução de problemas referentes a falhas e defeitos nos equipamentos ofertados;

1.3.9.1.2 Serviços relacionados a problemas no software do fabricante, como: bugs e indisponibilidades;

1.3.9.1.3 Os serviços de consultoria e suporte técnico a serem prestados não abrangem as atividades referentes à primeira instalação e configuração inicial de cada sistema objeto desta especificação técnica, conforme listado nos itens 07 e 08;

1.3.9.2 Serviços de Consultoria e Suporte Técnico, são aqueles que visam auxiliar a equipe técnica da CONTRATANTE na administração e operação do sistema, no âmbito das atividades que exijam conhecimentos com maior grau de complexidade e que possam impactar negativamente no negócio caso sejam executadas sem sucesso. Tal proposição encontra justificativa no fato de que o sistema se mostra razoavelmente complexo em função da quantidade de componentes de "software" especializados que são implementados no conjunto de "appliance" que compõem o sistema, sendo que o provimento de todo e qualquer serviço de TIC na rede mundial de computadores depende do nível de disponibilidade de tal plataforma.

1.3.9.3 Caberá à CONTRATADA a prestação dos serviços de consultoria e suporte técnico especializado a todos os produtos adquiridos ou que venham a ser utilizados pelo Tribunal de Justiça do Estado do Amazonas no que tange a cada sistema, pelo prazo de 36 (trinta e seis) meses, compreendendo suporte telefônico, remoto e local ("on-site", caso necessário) através de banco de horas.

1.3.9.4 A CONTRATADA deverá disponibilizar 500 (quinhentas) horas técnicas de consultoria e de suporte técnico ao longo do período de vigência do contrato, podendo estas ser utilizadas a qualquer tempo, mediante solicitação da CONTRATANTE.

1.3.9.5 Os serviços serão solicitados sob demanda, mediante a abertura de chamado efetuada por técnicos do Departamento de Informática do TJAM, via chamada telefônica, por e-mail ou plataforma de chamados da CONTRATADA, em Jornada de Horário Comercial (JHC), das 9h às 19h (horário de Brasília), de segunda a sexta-feira (8x5), informando a modalidade de atendimento no momento da solicitação.

1.3.9.6 Os serviços serão remunerados de acordo com a quantidade de horas necessárias para a execução de um conjunto de atividades previamente determinadas e aprovadas pela CONTRATANTE.

1.3.9.7 As horas utilizadas no mês serão pagas no mês subsequente, mediante emissão de documento comprobatório da CONTRATADA e ateste de sua efetiva execução pelo gestor do contrato.

1.3.9.8 Os serviços prestados à CONTRATANTE e que não atendam aos padrões de conformidade técnica serão notificados à CONTRATADA com a devida justificativa, não sendo objeto de faturamento e sujeitando-se, ainda, a CONTRATADA às penalidades contratuais correspondentes.

1.3.9.9 As horas técnicas deverão ser prestadas por técnicos devidamente certificados para prestar serviços de consultoria no sistema ofertado.

1.3.9.10 A CONTRATADA deverá prestar os serviços orientando-se pelos seguintes objetivos:

1.3.9.10.1 Utilização das melhores práticas recomendadas pela área de Segurança da Informação.

1.3.9.10.2 Adoção das melhores práticas para assegurar os melhores níveis de desempenho tecnicamente possíveis no que tange aos diversos módulos do sistema.

1.3.9.10.3 Uso otimizado e eficiente dos recursos tecnológicos empregados pelos diversos módulos do sistema.

1.3.9.10.4 Assegurar o melhor grau de integração entre os módulos do sistema e componentes de outros sistemas computacionais dos quais dependa seu bom funcionamento.

1.3.9.11 Os serviços de suporte técnico deverão ser prestados em plena conformidade com as seguintes condições:

1.3.9.11.1 O suporte técnico será realizado na modalidade remota, a contar o SLA a partir do momento em que a CONTRATANTE realizar a abertura de chamado.

1.3.9.12 A prestação dos serviços de suporte técnico por meio telefônico e por e-mail deverá contemplar, no mínimo:

1.3.9.12.1 SLA (Service Level Agreement): Acordo de nível de serviço entre a CONTRATANTE e a CONTRATADA, com base em categorias de serviços.

1.3.9.12.2 Incidente: Parada não planejada, indisponibilidade ou baixa performance de um serviço. Quando é aplicada uma solução de contorno, o incidente é concluído e aberto um Problema para investigação da causa raiz.

1.3.9.12.3 Solicitação de Serviço: Implementação, alteração e remoção de configuração de um serviço, que não tenha impacto no negócio.

1.3.9.13 Os SLAs praticados durante a vigência deste contrato são listados abaixo, bem com o critério de Classificação dos Chamados:

Categoria	**Urgência**	**SLA de 1ª Resposta**	**SLA de Solução**	**Descrição**
Incidente	Alta	2 horas	6 horas	Sistema indisponível ou com severa degradação de desempenho
Incidente	Média	8 horas	24 horas	Sistema disponível, com mau funcionamento, que importe baixa degradação de desempenho ou comprometimento em um de seus elementos que importe em risco para a disponibilidade do sistema;
Incidente	Baixa	24 horas	96 horas	Incidente que não afeta a operação e não gera impacto no negócio.
Solicitação de Serviço	Padrão	24 horas	N/A	Solicitação de serviços que não geram impacto ao negócio.

1.3.9.14 Entende-se como resolução de Incidente a aplicação de soluções paliativas, e como tratativa de causa raiz, a tratativa do Problema.

1.3.9.15 O SLA será pausado quando o retorno depender de ação da CONTRATANTE ou do FABRICANTE.

1.3.9.16 Os SLAs listados neste documento são acordos estabelecidos entre a CONTRATANTE e a CONTRATADA, não correspondendo aos SLAs praticados pelo FABRICANTE.

1.3.9.17 Nos casos em que a CONTRATADA julgar necessário e houver a concordância do TJAM, o atendimento poderá ser realizado on-site na sede do Tribunal de Justiça do Estado do Amazonas.

1.3.9.18 O suporte remoto deverá contemplar, no mínimo:

1.3.9.18.1 Esclarecimento de dúvidas de utilização, administração e operação dos módulos do sistema fornecido e utilizado pelo contratante.

1.3.9.18.2 Possibilidade de solicitação de envio de procedimentos para viabilizar a resolução de problemas de utilização, administração e operação dos módulos do sistema fornecido e utilizado pelo contratante.

1.3.9.18.3 Fornecimento de orientação sobre a necessidade de realizar atualização de determinado módulo de "software" do sistema para viabilizar a resolução de problemas reportados.

1.3.9.18.4 Fornecimento de orientação para a utilização do suporte junto ao fabricante do sistema, visando o envio de correções dos produtos contratados e o acionamento de laboratório em caso de indisponibilidade de correções.

1.3.9.19 A prestação dos serviços de consultoria e suporte técnico compreenderá, entre outras atividades não enumeradas taxativamente:

1.3.9.19.1 Análise, elaboração e implantação de projetos que envolvam componentes de "software" em uso e os que venham a ser utilizados futuramente pelo contratante.

1.3.9.19.2 Auxílio na gestão de políticas de segurança, com foco na prevenção e combate de ameaças, abrangendo desde avaliação e projeto até a implementação tecnológica e resposta a incidentes de segurança.

1.3.9.19.3 Avaliação de vulnerabilidades e prevenção de ameaças no contexto do ambiente computacional do contratante.

1.3.9.19.4 Identificação e solução de problemas em componentes de "software" do sistema.

1.3.9.19.5 Instalação e configuração de componentes de "software" em servidores de rede, caso necessário.

1.3.9.19.6 Instalação e configuração de atualizações de "firmware" e "software" ("patches") nos módulos do sistema.

1.3.9.19.7 Implementação de mecanismos de controle de acesso disponíveis nos módulos de "software" do sistema, visando impedir a proliferação de ameaças identificadas para as quais não exista, no momento, mecanismo de proteção apropriado.

1.3.9.19.8 Auxílio na auditoria e análise de "logs".

1.3.10. A justifica para o quantitativo a ser adquirido encontra-se no Estudo Técnico Preliminar, anexo a este termo.

1.4. Caracterização do Objeto:

1.4.1. O objeto do presente Termo de Referência enquadra-se no conceito de serviços comuns nos termos da Lei nº 14.133/2021.

1.4.2. A contratação decorrente do Registro de Preços será realizada de acordo com a necessidade e conveniência do Tribunal de Justiça do Amazonas, mediante a emissão de requisição de fornecimento e da Nota de Empenho.

1.5. Fundamentação Legal:

1.5.1. A contratação deverá obedecer, no que couber, ao disposto na legislação a seguir:

a) Lei nº 14.133, de 1º de abril de 2021;

b) Resolução n.º 64/2023-TJAM, de 5 de dezembro de 2023.

1.5.2. Legislações aplicáveis ao objeto a ser contratado, no que couber:

a) Decreto nº 10.222/2020 (Estratégia Nacional de Segurança Cibernética);

b) Lei nº 12.965/2014 (Marco Civil da Internet) - art. 10º e 11º;

c) Decreto nº 8.135/2013 (Comunicações de Dados da APF);

d) Instrução Normativa SGD/ME nº 1/2019 (Contratação de TIC);

e) Instrução Normativa SLTI/MP nº 1/2010;

f) Portaria SEGES/ME nº 8.678/2021 (Governança de TIC);

g) Resolução CNJ nº 185/2013 (Política Nacional de Segurança do PJe);

h) Normas ABNT NBR ISO/IEC 27001, 27002, 27005;

i) Resolução 468/2022-CNJ.

1.6. Indicação de necessidade de apresentação de amostras, catálogos, manuais, folders ou prospectos:

1.6.1. Para este certame, não será exigida apresentação de amostras, catálogos, manuais, folders ou prospectos.

1.7. Valor estimado da contratação:

1.7.1. A estimativa de valor da contratação será discriminada no Mapa de Preços a ser elaborado pela Divisão de Compras e Operações.

1.7.2. Tabela exemplificativa de cotação:

GRUPO	ITEM	ESPECIFICAÇÕES	QUANTIDADE MÍNIMA POR CONTRATAÇÃO	QUANTIDADE TOTAL	UND	PREÇO (R$)	PREÇO TOTAL (R$)
01	**Renovação e atualização da Solução F5 BIG-IP i5800 Best Bundle com IP Intelligence**						
	1	Renovação da garantia F5 BIG-IP i5800 Best Bundle (com IP Intelligence) suporte Premium 24x7 pelo período de 06 (seis) meses.	01	01	conjunto	R$	R$
	2	Atualização/substituição do appliance da solução i5800 para a linha r5800 pelo período de 36 (trinta e seis) meses	02	02	unidade	R$	R$
	3	Licenciamento Best Bundle (com IP Intelligence) e suporte Premium 24x7 pelo período de 36 (trinta e seis) meses	02	02	unidade	R$	R$
02	**Expansão módulos Distributed Cloud e Nginx**						
	4	Licença Base – Distributed Cloud Base Package pelo período de 36 (trinta e seis) meses	01	01	unidade	R$	R$
	5	Licença F5 NGINX ONE por instância com suporte Premium 24x7 pelo período de 36 (trinta e seis) meses	01	01	unidade	R$	R$
	6	Licença F5 NGINX ONE por node com suporte Premium 24x7 pelo período de 36 (trinta e seis) meses	01	04	unidade	R$	R$
03	**Serviços de Implantação**						
	7	Serviço de migração e atualização linha “i” 5800 para “r”5800	01	01	unidade	R$	R$
	8	Serviço de implantação da solução Base Package (item 4)	01	01	unidade	R$	R$
	9	Serviço de implantação da solução NGINX ONE (item 05 e/ou 06)	01	01	unidade	R$	R$
	10	Serviços de Consultoria e/ou Suporte Técnico (banco de horas)	100	500	hora	R$	R$
VALOR TOTAL ESTIMADO DO SRP						**R$**	

1.8. Adequação orçamentária:

1.8.1. A contratação pretendida está prevista no Plano de Contratação Anual 2025, sob o Código **SETIC-2025-67**.

2. CONDIÇÕES GERAIS DA CONTRATAÇÃO

2.1. O objeto deste Termo de Referência caracteriza-se como situação prevista na modalidade Pregão, sob a forma Eletrônica, nos termos do artigo 28, inciso I da, Lei nº 14.133/2021.

2.2. A presente contratação adotará como regime de execução a Empreitada por Preço Unitário.

2.3. O procedimento para a contratação pretendida neste instrumento será regido pelo Sistema de Registro de Preços, conforme apontado na escolha da solução do Estudo Técnico Preliminar.

2.4. O critério de julgamento será o de **MENOR PREÇO.**

2.5. O critério de adjudicação da contratação será GLOBAL, levando em consideração o prejuízo de ordem técnica que poderia ocorrer caso os serviços fossem prestados por diferentes empresas, uma vez que os serviços a serem contratados guardam estreita relação entre si e dependem de forte integração para que sejam efetivos e alcancem os resultados pretendidos.

2.6. Participação de consórcios de empresas:

2.6.1. A participação de consórcios no certame que se originará do presente Termo de Referência não será permitida, em razão da complexidade e o vulto do objeto não limitarem a participação de fornecedores aptos a executar o objeto. Os potenciais fornecedores, em sua maioria, dispõem de condições de participar isoladamente do certame e prestar a integralidade do objeto, não sendo o caso de permitir a junção de esforços de 2 (duas) ou mais empresas para a execução da contratação pretendida. Nesse caso, a possibilidade de participação de consórcios poderia limitar a competitividade do certame, uma vez que se admitiria que empresas se associassem e não disputassem individualmente o objeto da licitação.

2.7. Não será permitida a subcontratação do objeto deste Termo de Referência.

2.8. Tratamento diferenciado para Microempresas, Empresas de Pequeno Porte ou Cooperativas:

2.8.1. Aplicam-se a este certame, no que couber, as disposições constantes dos arts. 42 a 49 da Lei Complementar nº 123, de 14 de dezembro de 2006.

3. REQUISITOS DO FORNECEDOR

3.1. Vistoria:

3.1.1. Para a execução do objeto, não será necessária realização de vistoria.

3.2. Qualificação Técnica:

3.2.1. Qualificação técnico-profissional: a qualificação técnico-profissional se refere às pessoas físicas que prestam serviços à empresa licitante.

3.2.1.1. Comprovação de que a contratada dispõe de, no mínimo, 01 profissional certificado em soluções F5, tais como F5 Certified BIG-IP Administrator ou equivalente, com documento a ter conformidade aferida pela SETIC.

3.2.1.2. Tal comprovação deverá ser apresentada somente no momento da assinatura contrato, conforme Estudo Técnico Preliminar.

3.2.2.Qualificação técnico-operacional: a qualificação técnico-operacional diz respeito à empresa que pretende executar o objeto licitado.

3.2.2.1. Para o objeto a ser licitado, será necessária a apresentação dos seguintes documentos relativos a qualificação técnico-operacional:

3.2.2.1.1. Apresentação de, no mínimo, um atestado de capacidade técnica emitido por pessoa jurídica de direito público ou privado, que comprove experiência no fornecimento, implantação ou suporte de soluções F5 voltadas à segurança de aplicações web (WAF) e balanceamento de carga, demonstrando aptidão técnica na prestação de serviços relacionados à referida tecnologia.

3.2.2.1.1.1. Não será exigido um quantitativo mínimo de atestados, nem quantitativo mínimo de bens ou serviços do objeto licitado, uma vez que a análise da capacidade técnica priorizará a qualidade dos serviços já executados, a experiência com objetos similares e a adequação aos prazos e condições da licitação.

3.2.2.1.2. Apresentação de certificação de competência e de revenda autorizada, emitida pelo fabricante F5 Networks.

3.2.2.1.3. No caso de pessoa jurídica de direito público, o(s) atestado(s) ou certidão(ões) deverá(ão) ser assinado(s) pelo responsável do setor competente do órgão, preferencialmente munidos de mecanismos de verificação ou autenticação.

3.2.2.1.4. No caso de pessoa jurídica de direito privado, o(s) atestado(s) ou certidão(ões) deverá(ão) conter dados suficientes para identificação civil do declarante, com referência ao cargo/função que ocupa na empresa e formas de contato, ou munidos de mecanismos de verificação ou autenticação.

3.2.2.1.5. Os documentos apresentados poderão ser objeto de diligências, a critério da Administração.

3.2.3. As exigências e condições estabelecidas são pertinentes e razoáveis para a garantia de que o objeto licitado tenha a qualidade desejada.

3.2.4. As exigências relativas à capacidade técnica, seja ela de caráter técnico-profissional ou técnico-operacional, guardam amparo constitucional e não constituem, por si só, restrição indevida ao caráter competitivo de uma licitação.

4. MODELO DE GESTÃO

4.1. A fiscalização do objeto será realizada pela Secretaria de Tecnologia da Informação e Comunicação - SETIC

4.1.1. A execução do objeto deverá ser acompanhada e fiscalizada por servidor designado como responsável ou por seu substituto.

4.1.2. A SETIC será responsável pela avaliação da conformidade dos materiais/equipamentos, e anotará em registro próprio todas as ocorrências relacionadas à falhas ou problemas observados, determinando o que for necessário à regularização das mesmas.

4.1.3. A existência da fiscalização de nenhum modo diminui ou altera a responsabilidade do fornecedor na total execução do objeto.

4.1.4. Deverá ser mantido preposto, aceito pela CONTRATANTE, durante o período de execução do objeto, para representá-lo sempre que for necessário.

4.2. As comunicações entre o órgão e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica (e-mail) para esse fim.

4.3. Indicação de instrumento para efetivar a contratação:

4.3.1 Será necessária a formalização de contrato para a execução do serviço objeto desse termo.

4.3.2. Após a assinatura do contrato, o órgão poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

4.4. Vigência contratual:

4.4.1 A vigência do contrato a ser firmado será de 36 (trinta e seis) meses, podendo ser prorrogada, desde que justificadamente, pelo prazo necessário à conclusão do objeto, conforme Art. 6º, XVII, da Lei Federal n.° 14.133/2021.

4.4.2. Os prazos de execução deverão seguir as previsão estabelecidas no Estudo Técnico Preliminar:

4.4.2.1. **06 (seis) meses** para a eventual renovação da garantia F5 BIG-IP i5800 Best Bundle (com IP Intelligence) suporte Premium 24x7, item 01;

4.4.2.2. **36 (trinta e seis) meses** para os licenciamentos e para a eventual atualização/substituição do appliance i5800 pela linha r5800.

4.5. Índice de reajuste:

4.5.1. Os preços contratados poderão ser reajustados, após solicitação da CONTRATADA, observado o interregno mínimo de 12 (doze) meses, tendo como limite máximo a variação do Índice de Custos de Tecnologia da Informação - ICTI, ocorrida nos últimos 12 (doze) meses.

4.5.2. O interregno mínimo de 12 (doze) meses será contado a partir da data orçamento estimado, assim considerada a data de conclusão da apuração do valor estimado da contratação, ou, da planilha orçamentária, independentemente da data da tabela ou sistema referencial de custos utilizado.

4.5.3. Nos reajustamentos subsequentes ao primeiro, o interregno mínimo de 12 (doze) meses será contado da data de início dos efeitos financeiros do último reajustamento ocorrido.

4.5.4. O reajuste deverá ser solicitado antes do término da atual vigência deste Contrato, sob pena de preclusão.

4.6. Da Ata de Registro de Preços:

4.6.1. Será necessária a formalização de Ata de Registro de Preços.

4.6.2. O prazo de vigência da ata de registro de preços será de 1 (um) ano e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso.

4.6.2.1. Na renovação, que trata o item anterior, os itens da ATA serão renovados em sua integralidade e totalidade.

4.6.3. Os órgãos e entidades poderão aderir à ata de registro de preços na condição de não participantes, observados os seguintes requisitos:

I - apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

II - demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado;

III - prévias consulta e aceitação do órgão ou entidade gerenciadora e do fornecedor.

4.6.4. A faculdade de aderir à ata de registro de preços na condição de não participante poderá ser exercida:

I - por órgãos e entidades da Administração Pública federal, estadual, distrital e municipal, relativamente a ata de registro de preços de órgão ou entidade gerenciadora federal, estadual ou distrital; ou

4.6.5. As aquisições ou as contratações não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o órgão gerenciador e para os órgãos participantes.

4.6.6. O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que aderirem.

5. OBRIGAÇÕES DA CONTRATADA E DO CONTRATANTE.

5.1. São obrigações e responsabilidades do CONTRATANTE:

5.1.1. Efetuar os pagamentos nas condições e preços pactuados.

5.1.2. Promover o acompanhamento e a fiscalização da execução do objeto, sob os aspectos quantitativos e qualitativos, anotando em registro próprio as faltas detectadas e comunicando à empresa as ocorrências de qualquer fato que, a seu critério, exija medidas por parte daquela.

5.1.3. Rejeitar, no todo ou em parte, os materiais entregues em desacordo com as exigências deste Termo.

5.1.4. Notificar por escrito a ocorrência de eventuais imperfeições na execução do objeto, fixando prazo para a sua correção.

5.1.5. Proporcionar todas as facilidades para que ocorra a correta execução do objeto.

5.1.6. Comunicar qualquer irregularidade ou ilegalidade encontrada no fornecimento do objeto.

5.1.7. Prestar as informações e os esclarecimentos atinentes à execução do objeto que venham a ser solicitados.

5.1.8. Solicitar o fornecimento do objeto deste Termo de Referência.

5.1.9. Fiscalizar e acompanhar a execução da Ata de Registro de Preços.

5.1.10. Manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

5.1.11. Demais obrigações estipuladas no Contrato.

5.2. São obrigações e responsabilidades da CONTRATADA:

5.2.1. Executar o objeto desta contratação, atendendo às especificações estabelecidas neste Termo de Referência e as quantidades indicadas no instrumento contratual.

5.2.2. Manter todas as condições de habilitação e qualificação exigidas na licitação em compatibilidade com as obrigações assumidas.

5.2.3. Responsabilizar-se única e exclusivamente pelo pagamento de todos os encargos e demais despesas, diretas ou indiretas, decorrentes da execução do objeto do presente Termo de Referência, tais como impostos, taxas, contribuições fiscais, previdenciárias, trabalhistas, fundiárias; enfim, por todas as obrigações e responsabilidades, sem qualquer ônus adicional ao CONTRATANTE.

5.2.4. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho quando, em caso de ocorrência, forem vítimas seus empregados no desempenho dos serviços ou em conexão com eles, ainda que ocorridos nas dependências do CONTRATANTE.

5.2.5. Cumprir os normativos e os procedimentos definidos pelo CONTRATANTE.

5.2.6. Primar pelo bom planejamento das atividades, utilizar as boas práticas e técnicas de governança, avaliar previamente a viabilidade técnica, os riscos e os impactos de suas ações.

5.2.7. Realizar a entrega do objeto em conformidade com os horários e períodos determinados pelo CONTRATANTE.

5.2.8. Submeter seus profissionais aos regulamentos de segurança e disciplina instituídos pelo CONTRATANTE, durante o tempo de permanência nas suas dependências.

5.2.9. Comunicar às unidades do CONTRATANTE responsáveis pela fiscalização do objeto, por escrito, qualquer anormalidade, bem como atender prontamente o que lhe for solicitado e exigido.

5.2.10. Responder por todas as despesas decorrentes do fornecimento.

5.2.11. Refazer todos os serviços que, a juízo do representante do CONTRATANTE, não forem considerados satisfatórios, sem que caiba qualquer acréscimo no custo contratado.

5.2.12. Não realizar, promover e incentivar a divulgação de qualquer dado ou informação do ambiente do CONTRATANTE.

5.2.13. Obedecer às normas internas do CONTRATANTE, relativas à segurança, à identificação, ao trânsito e à permanência de pessoas em suas dependências.

5.2.14. Manter sigilo e ciência das normas de segurança e privacidade vigentes no órgão, se responsabilizando por todos os seus empregados diretamente envolvidos na contratação.

5.2.15. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste contrato, devendo orientar seus profissionais nesse sentido.

5.2.16. Tratar todas as informações a que tenha acesso, em caráter de estrita confidencialidade, não podendo, sob qualquer pretexto, divulgar, revelar, reproduzir, ou delas dar conhecimento a terceiros estranhos a esta contratação, bem como utilizá-las para fins diferentes dos previstos na presente contratação.

5.2.17. Acatar as determinações feitas pela fiscalização do CONTRATANTE no que tange ao cumprimento do objeto.

5.2.18. Prestar, de imediato, todos os esclarecimentos solicitados pela fiscalização do CONTRATANTE no que diz respeito a execução do objeto.

5.2.19. Fornecer os materiais, observadas rigorosamente as especificações constantes no Termo de Referência.

5.2.20. Observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios.

5.2.21. Responder pelos vícios e defeitos dos materiais e serviços e assumir os gastos e as despesas que se fizerem necessários para adimplemento das obrigações decorrentes da execução do objeto.

5.2.22. Responsabilizar-se por danos causados ao patrimônio do CONTRATANTE, ou de terceiros, ocasionados por seus profissionais, em virtude de dolo ou culpa, durante a execução do objeto.

5.2.23. Notificar, formal e tempestivamente, a CONTRANTE sobre quaisquer irregularidades e inconformidades observadas durante a execução do objeto, bem como qualquer ocorrência relativa ao comportamento de seus empregados, quando em atendimento, que venha a ser considerada prejudicial ou inconveniente para a CONTRATADA.

5.2.24. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo CONTRATANTE necessários à perfeita execução do objeto.

5.2.25. Manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

5.2.26. Demais obrigações estipuladas no Contrato.

6. REGIME DE EXECUÇÃO

6.1. A execução do objeto deste Termo de Referência será sob demanda.

6.2. A solicitação para início da execução dos serviços será com a expedição da Ordem de Serviço. A comunicação será realizada por e-mail.

6.3. Os serviços deverão ser executados conforme diretrizes estabelecidas na Ordem de Serviço.

6.4. O objeto deste Termo de referência será recebido da seguinte forma:

6.4.1. **Provisoriamente**, no prazo de 05 dias corridos, pelo responsável por seu acompanhamento e fiscalização, mediante termo detalhado, quando verificado o cumprimento das exigências de caráter técnico.

6.4.2. **Definitivamente**, no prazo de 10 dias úteis, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais.

6.4.3. O objeto será recusado caso não atenda as especificações técnicas solicitadas no Termo de Referência, devendo a empresa providenciar os ajustes necessários para adequação, em um prazo de 05 dias corridos contados a partir da comunicação, quando do não aceite.

6.4.4. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

6.4.5. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do objeto.

6.5. Garantia ou assistência técnica.

6.5.1. Esta pretensa contratação, por envolver a renovação do licenciamento da solução F5 BIG-IP i5800 Best Bundle com o módulo IP Intelligence, conforme descrito no item 6.4.1 – Grupo 1, garantirá a continuidade do suporte técnico especializado, o acesso às atualizações de software e a manutenção da alta disponibilidade e segurança das aplicações críticas sob responsabilidade do TJAM.

6.5.2. Os serviços de manutenção e suporte técnico especializado a serem prestados deverão incluir, no mínimo:

6.5.2.1. Suporte Técnico Remoto e Presencial: Atendimento técnico especializado para diagnóstico e resolução de incidentes relacionados às soluções F5, com suporte disponibilizado por meio de canais oficiais (telefone, e-mail e portal de chamados), conforme os níveis de serviço (SLA) definidos contratualmente, inclusive com disponibilidade 24x7 para casos críticos, quando aplicável.

6.5.2.2. Correção de Defeitos e Atualizações de Software: Disponibilização contínua de atualizações corretivas, evolutivas e de segurança dos componentes licenciados, garantindo que o ambiente permaneça atualizado, protegido contra novas vulnerabilidades e em conformidade com as recomendações e melhores práticas do fabricante.

6.5.2.3. Substituição de Equipamentos Defeituosos (RMA): Execução de procedimentos de substituição de hardware defeituoso (quando aplicável), por meio de envio de peças de reposição originais homologadas pelo fabricante, dentro dos prazos estabelecidos em contrato, de modo a assegurar a continuidade dos serviços e mitigar impactos operacionais.

6.6. Na contratação de serviços de natureza intelectual ou outro em que seja identificada essa necessidade, deverá ser estabelecido como obrigação da contratada realizar a transição contratual com transferência de conhecimento, tecnologia ou técnica empregadas, sem perda de informações, podendo ser exigida, inclusive, a capacitação dos técnicos da administração.

6.6.1. A transição contratual deverá prever a transferência de conhecimento e tecnologia, promovendo uma relação mais transparente e colaborativa entre as partes. Essa transferência é essencial para:

6.6.1.1. Capacitar a equipe interna do TJAM a operar e manter a solução de forma autônoma;

6.6.1.2. Minimizar o tempo de resposta a incidentes;

6.6.1.3. Reduzir a dependência de suporte externo;

6.6.1.4. Manter a continuidade operacional com qualidade e segurança.

7. PENALIDADES POR DESCUMPRIMENTO CONTRATUAL

7.1. Poderão ser aplicadas à CONTRATADA que incorrer nas infrações previstas neste Termo de Referência, no Edital de Licitação, no Contrato Administrativo e na Ata de Registro de Preços, as seguintes sanções:

a) advertência;

b) multa;

c) impedimento de licitar e contratar;

d) declaração de inidoneidade para licitar ou contratar.

7.2. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas cumulativamente com a sanção de multa.

7.3. A sanção de impedimento de licitar e contratar com o ente federativo não poderá ser aplicada cumulativamente com a de declaração de inidoneidade.

7.4. A aplicação das sanções acima previstas não exclui a obrigação de reparação integral do dano causado à administração pública.

7.5. As infrações e sanções administrativas observarão os termos de cláusula específica da Minuta Contratual.

8. ADOÇÃO DE IMR OU ANS

8.1. Não se aplica.

9. FORMA DE PAGAMENTO

9.1. O pagamento será efetuado em até 30 (trinta) dias, mediante apresentação da Nota Fiscal/Fatura, após ser devidamente atestada a sua conformidade pelo Fiscal designado para acompanhar e fiscalizar a execução.

9.1.1. As licenças serão pagas integralmente e suas execução irão viger conforme os prazos de execução estabelecidos na contratação.

9.1.2. O item de horas técnicas, será pago conforme demanda e a efetiva execução.

9.2. O pagamento será efetuado por meio de Ordem Bancária Eletrônica em conta corrente indicada na Nota Fiscal/Fatura, devendo, para isso, ficar explícito o nome do banco, agência, localidade e número da conta corrente em que deverá ser efetivado o crédito.

9.3. Caso a CONTRATADA seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, a mesma deverá apresentar, juntamente com a Nota Fiscal/Fatura, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

9.4. Para a efetivação do pagamento deverão ser mantidas as mesmas condições iniciais de habilitação, cumpridos os seguintes requisitos: Comprovação da regularidade fiscal da CONTRATADA para com a Fazenda Federal, Estadual e Municipal; Comprovação da regularidade fiscal da CONTRATADA relativa à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei; Comprovação de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas (CNDT); Comprovação de regularidade junto ao Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis); e o Cadastro Nacional de Empresas Punidas (Cnep).

9.5. A Nota Fiscal/Fatura correspondente será examinada diretamente pelo Fiscal designado pela CONTRATANTE, o qual somente atestará a prestação do serviço contratado e liberará a referida Nota Fiscal/Fatura para pagamento quando cumpridas, pela CONTRATADA, todas as condições pactuadas.

9.6. Havendo erro na Nota Fiscal/Fatura ou circunstância que impeça a liquidação da despesa, aquela será devolvida pelo Fiscal à CONTRATADA e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento será interrompido e reiniciado a partir da regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para o CONTRATANTE.

9.7. O pagamento observará, ainda, as demais disposições contidas em Cláusula específica da Minuta Contratual.

9.8. Considerando que a execução dos serviços será sob demanda, os pagamentos serão realizados para os itens efetivamente prestados, mediante apresentação da Nota Fiscal da empresa.

10. GARANTIA CONTRATUAL

10.1. A CONTRATADA deverá apresentar ao CONTRATANTE, em até 05 (cinco) dias úteis, contados da assinatura do contrato, comprovante de garantia, no valor correspondente a 5% (cinco por cento) do valor total do contrato, cabendo-lhe optar por uma das modalidades de garantia prevista no art. 96, § 1º da Lei n.º 14.133/2021.

10.2. A garantia deverá ser prestada com vigência de 03 (três) meses após o término da vigência do Contrato e será restituída automaticamente, ou por solicitação, no prazo de até 60 (sessenta) dias contados do final da vigência do contrato ou da rescisão, somente após comprovação de que a empresa pagou todas as verbas rescisórias trabalhistas decorrentes da contratação.

10.2.1. Caso a CONTRATADA não efetive o cumprimento das obrigações previstas no subitem anterior, a garantia será utilizada para o pagamento dessas verbas trabalhistas diretamente pelo CONTRATANTE.

10.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

10.3.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

10.3.2. Multas moratórias e punitivas aplicadas pela Administração à contratada; e

10.3.3. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

10.4. Quando a garantia for apresentada em dinheiro, ela será atualizada monetariamente, conforme os critérios estabelecidos pela instituição bancária em que for realizado o depósito.

10.5. Quando a opção da garantia for a modalidade de seguro-garantia, a apólice deverá conter cláusulas específicas, oferecendo cobertura para despesas com obrigações contratuais e riscos trabalhistas, bem como multas que tenham caráter punitivo.

10.6. Aditado o Contrato, prorrogado o prazo de sua vigência ou alterado o seu valor, fica a CONTRATADA obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e modalidades constantes desta cláusula. Nesses casos, a garantia será liberada após a apresentação da nova garantia e da assinatura do termo aditivo ao Contrato.

10.7. Nas hipóteses em que a garantia for utilizada total ou parcialmente – como para corrigir quaisquer imperfeições na execução do objeto do contrato ou para reparar danos decorrentes da ação ou omissão da CONTRATADA, de seu preposto ou de quem em seu nome agir, ou ainda nos casos de multas aplicadas depois de esgotado o prazo recursal – a CONTRATADA deverá, no prazo de 03 (três) dias, recompor o valor total dessa garantia, sob pena de aplicação de penalidades previstas neste Contrato.

10.8. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

11. CLÁUSULAS GERAIS DE SUSTENTABILIDADE

11.1. A empresa contratada deverá contribuir para a promoção do desenvolvimento nacional sustentável, em conformidade com o artigo 225 da Constituição Federal de 1988 e o artigo 5º da Lei nº 14.133/21, observando os princípios da eficiência, economicidade e sustentabilidade ambiental, social e econômica.

11.2. Adicionalmente, a contratada deverá, sempre que viável, observar as normas vigentes relacionadas à sustentabilidade ambiental e aderir às melhores práticas delineadas no Guia Prático de Critérios de Sustentabilidade para Compras no TJAM e no Guia Nacional de Contratações Sustentáveis da AGU, durante a execução dos serviços.

11.3. Cabe à contratada demonstrar ações para reduzir emissões de gases de efeito estufa em suas operações, como investir em tecnologias e práticas que reduzam o consumo de energia, adotar práticas de gestão adequada de resíduos, promover práticas de governança sustentável, reduzir o consumo de combustíveis fósseis e seus derivados.

11.4. Recomenda-se que a contratada cumpra as cotas raciais, de gênero e de pessoas com deficiência, conforme estabelecido pela legislação vigente, incluindo o Decreto Federal nº 11.430/2023.

11.5. Recomenda-se exigir da contratada um programa interno de treinamento visando à redução de consumo de energia elétrica, consumo de água e produção de resíduos sólidos, alinhado às melhores práticas de sustentabilidade.

11.6. Estabelecer a separação adequada e o descarte responsável de resíduos, incluindo a reciclagem de materiais quando aplicável, em conformidade com a Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010) e a Resolução nº 307/2002 do CONAMA.

11.7. Incentivar a redução de resíduos por meio de práticas de consumo consciente, promovendo a educação ambiental entre os colaboradores e fornecedores.

11.8. Fornecer aos empregados os equipamentos de segurança necessários para a execução dos serviços e fiscalizar o uso, conforme as Normas Regulamentadoras do Ministério do Trabalho e Emprego.

11.9. Realizar a separação dos resíduos recicláveis descartados em função de seus serviços, conforme as diretrizes estabelecidas pela Associação Brasileira de Normas Técnicas (ABNT).

11.10. Respeitar as Normas Brasileiras (NBR) publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos, garantindo a conformidade com as melhores práticas de gestão de resíduos.

11.11. No que diz respeito à gestão de resíduos, a contratada deverá aderir às diretrizes estabelecidas na Lei nº 12.305/2010 - Política Nacional de Resíduos Sólidos, na Resolução nº 307/2002 do Conselho Nacional de Meio Ambiente (CONAMA), e na Instrução Normativa SLTI/MPOG nº 1/2010. A contratada assumirá como obrigações a aplicação de critérios e práticas sustentáveis, incorporando-as como especificações técnicas do objeto.

11.12. Os serviços a serem contratados devem possuir critérios e práticas de sustentabilidade em relação aos materiais e produtos a serem empregados, bem como a previsão da adequada execução a fim de atender às demandas sem infringir a legislação ambiental aplicável. A contratada deverá racionalizar o uso de substâncias potencialmente tóxicas ou poluentes, informando, se for o caso, o tratamento adotado para o recolhimento dos resíduos; substituir as substâncias tóxicas por outras atóxicas ou de menor toxicidade. Os materiais empregados pela empresa deverão atender à melhor relação entre custo e benefício, considerando os impactos ambientais, positivos e negativos, associados ao produto.

11.13. A contratada assumirá a responsabilidade ambiental por toda a execução dos serviços, notadamente quanto ao descarte correto dos resíduos gerados, devendo manter-se informada e atualizada acerca das normas que regem a matéria, principalmente as regras municipais.

11.13.1. Observar as leis municipais relacionadas ao transporte, resíduos volumosos e demais leis vigentes sobre o objeto do edital, bem como as particularidades das quais cerceiam o descarte de resíduos amparados pelo edital, não cabendo reclamações posteriores.

11.14. A contratada deverá adotar práticas de logística reversa, quando aplicável, para garantir o retorno adequado de produtos e embalagens ao ciclo produtivo, conforme estabelecido pela Política Nacional de Resíduos Sólidos.

11.15. Incentivar a adoção de tecnologias limpas e processos produtivos eficientes, visando à redução do impacto ambiental e ao uso racional dos recursos naturais.

12. RESPONSÁVEIS PELO TERMO DE REFERÊNCIA

12.1. Subscrevem o Termo de Referência os servidores responsáveis por sua elaboração, nos moldes e parâmetros estabelecidos pelo Tribunal de Justiça do Estado do Amazonas. Além da exigência legal da aprovação da autoridade competente, o instrumento em tela carece da ratificação de que retrata o que fora ordenado aos responsáveis por sua elaboração.

13. DOS ANEXOS

13.1. São partes integrantes deste Termo de Referência os seguintes anexos:

a) Mapa de Gerenciamento de Riscos na Contratação;

b) Estudo Técnico Preliminar;

c) Mapa de Preços.

Manaus, *data do sistema*

assinado digitalmente
Matheus Barreto dos Santos

Seção de Elaboração de Artefatos da Contratação