ESTUDO TÉCNICO PRELIMINAR - TJ/AM/SETIC/DVITIC

Responsáveis pela elaboração:

Diogo Mendonça de Sousa

Washington Alves da Cunha Neto

Contato: (92) 99239-1948

Número de identificação do ETP: 2317969

Categoria do Objeto: Serviços de Segurança da Informação.

CATSER: 27502

1. PLANO DE CONTRATAÇÕES ANUAL

1.1 O objeto da pretensa contratação, que consiste na renovação e atualização da solução do WAF F5, está previsto no Plano de Contratações Anual - PCA - do Poder Judiciário do Estado do Amazonas, sob o código **SETIC-2025-67**, conforme aprovado na **RESOLUÇÃO Nº 43, DE 22 DE OUTUBRO DE 2024** e disponibilizado no painel *BI* disponível NESTE LINK.

2. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

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.

2.2 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. Diante disso, a contratação revela-se imprescindível e está fundamentada nos seguintes aspectos:

2.2.1 Otimização do Tráfego e Balanceamento de Carga: O TJAM conta atualmente com 42 aplicações configuradas no F5 BIG-IP, que realizam o balanceamento inteligente de carga, redirecionando o tráfego de rede para os servidores mais adequados. Esse mecanismo assegura alta performance, melhora a experiência dos usuários e viabiliza a escala dinâmica do ambiente. Em caso de falha de servidores, o sistema realiza o redirecionamento automático do tráfego para servidores disponíveis, garantindo a continuidade dos serviços judiciais e a resiliência operacional do Tribunal.

2.2.2 Proteção Avançada de Aplicações: Das 42 aplicações em produção, 38 estão protegidas por Web Application Firewall (WAF), que atua de forma ativa na proteção contra ameaças catalogadas no OWASP Top 10, tráfego malicioso de bots e ataques de negação de serviço (DoS L7). Em 2024, o ambiente do TJAM bloqueou mais de 4.000.000 requisições ilegítimas, evidenciando a efetividade da proteção implementada. A não renovação comprometeria diretamente a capacidade de mitigação de ataques cibernéticos e exposição das aplicações judiciais a riscos severos de segurança.

2.2.3 Gestão Segura de Acessos (Access Policy Manager – APM): O módulo APM da solução viabiliza a centralização e a proteção de acessos a aplicações internas e APIs, sem a necessidade de VPN tradicional. Essa funcionalidade proporciona autenticação segura, acesso ágil e proteção avançada de credenciais institucionais, permitindo que servidores do TJAM acessem com segurança sistemas como Alvará, Precatórios, Helpdesk, Intranet, Senha, Gestão de Teletrabalho e outros. A ausência dessa camada de proteção acarretaria riscos adicionais de acesso não autorizado e comprometimento de dados sensíveis.

2.2.3.1 A estratégia da Secretaria de Tecnologia da Informação e Comunicação (SETIC) é reduzir progressivamente o uso de conexões VPN tradicionais, que representam pontos de vulnerabilidade e podem expor o ambiente a riscos cibernéticos. A substituição do modelo tradicional de VPN por acesso seguro via APM, com políticas de autenticação robustas (incluindo autenticação multifator e Single Sign-On), fortalece a segurança da infraestrutura de TI, minimiza a superfície de ataque e eleva o nível de resiliência cibernética do TJAM.

2.3 A prorrogação dos serviços de licenciamento assegura que o TJAM continuará a operar com uma solução de segurança cibernética de ponta, capaz de se adaptar rapidamente a novos vetores de ataque e demandas tecnológicas emergentes. A integração contínua do WAF F5 com a infraestrutura do TJAM maximiza o desempenho das aplicações e otimiza o uso dos recursos de TI, mantendo um alto padrão de serviço e segurança.

2.4 Para fins de compatibilidade e atualização do software mediante novas assinaturas e funcionalidades/recursos técnicos de segurança, faz-se necessária a atualização do appliance em utilização neste Tribunal para o novo modelo, ou seja, o hardware da linha “i” 5800, deverá ser substituído pela linha “r” e mantido o mesmo licenciamento – Best Bundle com IP Intelligence, conforme melhor prática sugerido pelo fabricante F5 Networks, em caso de vulnerabilidades que possam surgir a partir de 2027.

2.4.1 A expansão é justificada pela crescente exposição das aplicações institucionais do TJAM a ambientes de nuvem pública e privada, em consonância com a Resolução CNJ nº 370/2021, que recomenda a adoção segura e planejada de soluções de computação em nuvem como estratégia para a modernização tecnológica e o aumento da resiliência digital no Poder Judiciário. Além disso, a necessidade de proteção avançada de APIs, bem como a evolução arquitetural para ambientes modernos baseados em microserviços e APIs REST, reforçam a importância da expansão.

2.4.2 A adoção do NGINX One também trará benefícios diretos para o ambiente tecnológico do TJAM no que tange ao suporte a arquiteturas baseadas em contêineres e microserviços. O NGINX One é uma solução avançada que fornece gerenciamento centralizado, automação de configurações, balanceamento de carga, roteamento de APIs e proteção de tráfego para aplicações containerizadas, incluindo aquelas implementadas em plataformas Docker e orquestradores como Kubernetes

2.4.3 A solução F5 Distributed Cloud permitirá ao TJAM assegurar a proteção distribuída de aplicações contra ataques sofisticados, como DDoS, bots maliciosos e vulnerabilidades em APIs, enquanto o F5 NGINX proporcionará maior flexibilidade, escalabilidade e desempenho na entrega de aplicações e serviços críticos, alinhando-se às melhores práticas de segurança, disponibilidade e inovação tecnológica.

2.5 A renovação do licenciamento do F5 BIG-IP Best Bundle com o IP Intelligence, atualização da solução para linha “r” e a expansão da solução com F5 Distributed Cloud e F5 NGINX estão em total conformidade com as diretrizes da Resolução CNJ nº 468/2022, que disciplina as contratações de TIC no âmbito do Poder Judiciário; da Resolução CNJ nº 370/2021, que estabelece a necessidade de modernização da infraestrutura tecnológica e fortalecimento da resiliência cibernética no Poder Judiciário; e da Resolução CNJ nº 396/2021, que obriga a implementação de controles técnicos para a prevenção e resposta a incidentes de segurança. Além disso, a iniciativa está alinhada à Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), contribuindo diretamente para o fortalecimento da proteção de ativos críticos, a mitigação de ameaças cibernéticas e a elevação do nível de maturidade em segurança da informação no âmbito do TJAM.

3. UNIDADE DEMANDANTE

3.1 A unidade demandante responsável pelo desenvolvimento e acompanhamento deste estudo será a Secretaria de Tecnologia da Informação e Comunicação - SETIC.

4. REQUISITOS DA CONTRATAÇÃO

4.1 Trata-se da formação de Ata de Registro de Preços (ARP) para viabilizar a renovação do licenciamento e a expansão da Solução de Segurança F5 BIG-IP Best Bundle, com a inclusão dos módulos Distributed Cloud e NGINX, para garantir a proteção de aplicações e dados sensíveis, assegurando a continuidade dos serviços judiciais, especialmente em ambientes de transformação digital e computação em nuvem.

4.2 Sugere-se que a licitação seja realizada na Modalidade Pregão, na forma Eletrônica, tipo Menor Preço Global, mediante sistema de registro de preços.

4.3 Os eventuais acionamentos desta ARP resultarão em contratações por escopo, com vigência de 36 (trinta e seis) meses, conforme os seguintes prazos de execução:

4.3.1 06 (seis) meses para a eventual renovação da garantia F5 BIG-IP i5800 Best Bundle (com IP Intelligence) suporte Premium 24x7;

4.3.2 36 (trinta e seis) meses para os licenciamentos e para a eventual atualização/substituição do appliance da solução i5800 para a linha r5800.

4.4 A duração desses contratos poderá ser prorrogada, desde que justificadamente, pelo prazo necessário à conclusão do objeto, conforme Art. 6º, XVII, da Lei Federal n.° 14.133/2021.

4.5 Os equipamentos adquiridos devem atender a critérios de sustentabilidade, conforme orientações do *Guia Prático de Critérios de Sustentabilidade para Compras no TJAM*.

4.6 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:

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

4.6.2. Minimizar o tempo de resposta a incidentes;

4.6.3. Reduzir a dependência de suporte externo;

4.6.4. Manter a continuidade operacional com qualidade e segurança.

4.7. A contratada deverá fornecer treinamentos técnicos, documentação personalizada e suporte operacional para garantir a plena absorção dos conhecimentos relacionados a contratação pretendida.

4.8. A licitante deverá apresentar, na fase de habilitação, a seguinte documentação de qualificação técnica:

4.8.1. Comprovação de atividade econômica compatível com o objeto da contratação, por meio do CNAE correspondente.

4.8.2. 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;

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

4.9. No momento da assinatura do contrato, a licitante vencedora deverá comprovar que dispõe de no mínimo 01 profissional certificado em soluções F5, tais como F5 Certified BIG-IP Administrator ou equivalente.

4.10. Durante a transição contratual, a contratada deverá garantir a continuidade da prestação dos serviços, sem prejuízo à integridade, disponibilidade e segurança das informações do TJAM, realizando a migração de eventuais configurações e integrações necessárias de forma segura e controlada.

5. LEVANTAMENTO DE MERCADO E JUSTIFICATIVA DA ESCOLHA DO TIPO DE SOLUÇÃO A CONTRATAR

5.1. A necessidade de manter a padronização da infraestrutura de tecnologia e segurança do TJAM justifica a dispensa do levantamento de mercado para esta contratação. O Tribunal já possui uma arquitetura consolidada, baseada na solução F5 BIG-IP i5800 Best Bundle, que atua como plataforma central de proteção de aplicações, controle de acesso e balanceamento de carga. A adoção contínua dessa tecnologia garante interoperabilidade, eficiência operacional, segurança cibernética e escalabilidade do ambiente tecnológico. Essa justificativa encontra respaldo no art. 41, inciso I, alíneas "a" e "b", da Lei nº 14.133/2021, que permite a indicação de marcas e modelos específicos para manter a padronização e a compatibilidade com plataformas e padrões já adotados pela Administração.

5.2. A adoção de soluções ou tecnologias incompatíveis com o ambiente existente implicaria em aumento significativo de custos operacionais, administrativos e de segurança, além de comprometer a confiabilidade e a continuidade operacional dos serviços judiciais prestados. Alterações na arquitetura tecnológica exigiriam investimentos adicionais em capacitação, suporte, reconfiguração de aplicações, integração e migração, contrariando o princípio da eficiência administrativa.

5.3. A padronização da infraestrutura de tecnologia evita problemas de incompatibilidade entre sistemas, reduz a curva de aprendizado dos técnicos responsáveis pela administração da solução, facilita a integração entre os componentes existentes e novos módulos, e fortalece a governança de segurança da informação. Esse alinhamento com a infraestrutura já implantada também atende ao art. 47, inciso I, da Lei nº 14.133/2021, que determina que as licitações devem observar o princípio da padronização, garantindo compatibilidade técnica, estética e de desempenho.

5.4. A continuidade da tecnologia F5 BIG-IP i5800 Best Bundle através da renovação e atualização de hardware, minimiza riscos operacionais e mantém a eficiência da infraestrutura crítica do Tribunal, garantindo que as operações judiciais e administrativas permaneçam estáveis e seguras, sem necessidade de adaptações onerosas ou reestruturações técnicas desnecessárias. Dessa forma, a dispensa do levantamento de mercado se justifica não apenas pela necessidade de manter a padronização tecnológica do TJAM, mas também pelo respaldo legal conferido pela Lei nº 14.133/2021, garantindo economicidade, eficiência e continuidade dos serviços públicos.

5.5. Adicionalmente, a solução F5 BIG-IP i5800 Best Bundle e sua futura atualização para o novo modelo (linha r), assim como os módulos de expansão Distributed Cloud e NGINX, não se configuram como produtos de fornecedor único, sendo comercializados por diversos parceiros e revendedores autorizados no Brasil. Conforme verificado nos canais oficiais do fabricante F5 Networks e nas plataformas de seus parceiros certificados, há diversas empresas devidamente habilitadas para fornecer, implementar e prestar suporte à solução. Esse cenário garante a ampla competitividade no processo licitatório, promovendo a seleção da proposta mais vantajosa para a Administração Pública, em conformidade com os princípios da economicidade e isonomia.

5.6 Por fim, o objeto da contratação não apresenta complexidade técnica nem especificidades que justifiquem a convocação de audiência pública.

6. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

6.1 Em virtude do que foi exposto no item 5, 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.

6.2 Dessa forma, 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.

6.3 A renovação e a expansão visam assegurar a proteção contínua das aplicações críticas, otimizar o gerenciamento do tráfego de rede, modernizar a arquitetura tecnológica com foco em ambientes multicloud e APIs, além de garantir a conformidade com as normativas de segurança cibernética vigentes no âmbito do Poder Judiciário.

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

6.4.1 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.

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

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

Item	Descrição
1	Grupo 1 - Renovação da garantia F5 BIG-IP i5800 Best Bundle (com IP Intelligence) e atualização do appliance (hardware)
2	Grupo 2 - Expansão módulos Distributed Cloud e NGINX
3	Grupo 3 – Serviços de suporte técnico especializado e/ou consultoria

6.5 Licenciamento F5 BIG-IP Best Bundle com IP Intelligence (Grupo 01)

6.5.1 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.

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

6.5.2.1 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.

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

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

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

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

6.5.2.2 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.

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

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

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

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

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

6.5.2.3 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.

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

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

6.5.2.3.3 Proteção contra ataques DDoS dirigidos aos serviços de DNS.

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

6.5.2.4 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.

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

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

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

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

6.5.2.5 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.

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

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

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

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

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

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

6.5.3 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

6.6 Licenciamento F5 Distritbuted Cloud (Grupo 2)

6.6.1. Proteção de Aplicações Web e APIs

6.6.1.1 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;

6.6.1.2 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/);

6.6.1.3 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;

6.6.1.4 Suportar OCSP;

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

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

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

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

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

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

6.6.1.8 Permitir configurar monitores de disponibilidade de Origin Servers;

6.6.1.9 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;

6.6.1.9.1 Permitir definir políticas de WAF diferentes por pool;

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

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

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

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

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

6.6.1.12.3 Permitir enviar o certificado completo;

6.6.1.12.4 Permitir enviar atributos específicos do certificado;

6.6.1.13 Suportar HTTP/1.1 e HTTP/2;

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

6.6.1.14.1 Cross-Site Scripting (XSS);

6.6.1.14.2 Cross-Site Request Forgery (CSRF);

6.6.1.14.3 Directory Traversal;

6.6.1.14.4 Directory Climbing;

6.6.1.14.5 SQL injection;

6.6.1.14.6 Cookie Injection;

6.6.1.14.7 Command Injection;

6.6.1.14.8 Code Injection;

6.6.1.14.9 Web Parameter Tampering;

6.6.1.14.10 Cookie Tampering;

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

6.6.1.16 Implementar detecção e mitigação de violações do protocolo HTTP;

6.6.1.17 Implementar proteção contra exploração de vulnerabilidade (exploit);

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

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

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

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

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

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

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

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

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

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

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

6.6.1.29 Permitir desabilitar inspeções para tipos de ataques específicos;

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

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

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

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

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

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

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

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

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

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

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

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

6.6.1.41 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;

6.6.1.42 Permitir inserir cabeçalho HTTP na requisição e na resposta;

6.6.1.43 Permitir remover cabeçalhos HTTP da requisição;

6.6.1.44 Implementar o redirecionamento automático de HTTP para HTTPS;

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

6.6.1.46 Implementar mitigação automática de DDoS em camada 7;

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

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

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

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

6.6.2.3 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;

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

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

6.6.2.6 Implementar proteção de ataques à pilha TCP;

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

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

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

6.6.2.10 Permitir criar regras de respostas personalizadas;

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

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

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

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

6.6.2.14 Permitir configurar de mitigações específicas por aplicação;

6.6.2.15 Permitir configurar rate limit por aplicação;

6.6.2.16 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;

6.6.3 Implementar serviço DNS primário e secundário;

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

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

6.6.3.3 Possuir interface gráfica para gerenciamento de registros do DNS;

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

6.6.3.5 Implementar proteções de ataques direcionados aos serviços de DNS;

6.6.3.6 Implementar proteções de ataques de DDoS;

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

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

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

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

6.6.3.7.4 Permitir configurar topologias para respostas com base em geolocalização;

6.6.4 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;

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

6.6.4.2 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;

6.6.4.3 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;

6.6.4.4 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;

6.6.4.5 Permitir a criação de usuários com acesso à console;

6.6.4.6 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;

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

6.6.4.8 Permitir a configuração de Segundo Fator de Autenticação;

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

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

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

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

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

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

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

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

6.6.4.14 Deve ser compatível com mTLS;

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

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

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

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

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

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

6.6.4.20.1 Saúde geral da aplicação;

6.6.4.20.2 Latência fim a fim;

6.6.4.20.3 Estatísticas de TLS;

6.6.4.20.4 Eventos com origem, destino, ataque e ação;

6.6.4.20.5 Taxas de requisições, status code e métodos;

6.6.4.20.6 Latência e throughput da aplicação;

6.6.4.20.7 Total de requisições ao longo do tempo;

6.6.4.20.8 Lista de aplicações e requisições, ataques e bloqueios;

6.6.4.20.9 Tipos de eventos;

6.6.4.20.10 Ataques, origens e alvos mais comuns;

6.6.4.20.11 Assinaturas e violações mais comuns;

6.6.4.20.12 Sumário de segurança;

6.6.4.20.13 Classificação de bots das requisições;

6.6.4.20.14 Volume de requisições de bots e humanos;

6.6.4.20.15 Fluxos da aplicação mais atacados por bots;

6.6.4.20.16 Lista de bots maliciosos por origem IP e tipo;

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

6.6.4.20.18 Eventos de DDoS ao longo do tempo;

6.6.4.20.19 Taxa de requisições de ataques de DDoS;

6.6.4.20.20 Throughput do DDoS;

6.6.4.20.21 Mapa geográfico indicando a origem do DDoS;

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

6.6.4.20.23 Mapa geográfico das requisições de DNS por zona;

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

6.6.4.20.25 Lista de nomes de DNS mais solicitados;

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

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

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

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

6.6.4.23 Recursos Disponíveis por Unidade do Serviço de Base Package

6.6.4.23.1 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;

6.6.4.23.2 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;

6.6.4.23.3 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;

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

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

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

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

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

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

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

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

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

6.6.4.23.12.1 30 (trinta) dias para métricas de desempenho e eventos de auditoria;

6.6.4.23.12.2 07 (sete) dias para eventos de requisições e segurança;

6.6.4.23.12.3 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.

6.7 Licenciamento F5 NGINX (Grupo 2)

6.7.1. Características técnicas
6.7.1.1. Deve ser compatível com, pelo menos, os seguintes ambientes:
6.7.1.1.1. Bare metal
6.7.1.1.2. Container
6.7.1.1.3. Public cloud: AWS, Google Cloud Platform, Microsoft Azure
6.7.1.1.4. Virtual machine

6.7.1.2. Deve ser suportado, em pelo menos, nos seguintes sistemas operacionais:
6.7.1.2.1. Alpine Linux
6.7.1.2.1.1. 3.12 (x86_64, aarch64)
6.7.1.2.1.2. 3.13 (x86_64, aarch64)
6.7.1.2.1.3. 3.14 (x86_64, aarch64)
6.7.1.2.1.4. 3.15 (x86_64, aarch64)

6.7.1.2.2. Amazon Linux 2
6.7.1.2.2.1. LTS (x86_64, aarch64)

6.7.1.2.3. CentOS
6.7.1.2.3.1. 7.4+ (x86_64, aarch64, ppc64le)
6.7.1.2.3.2. 8.1+ (x86_64, aarch64, s390x)

6.7.1.2.4. Debian
6.7.1.2.4.1. 10 (x86_64, aarch64)
6.7.1.2.4.2. 11 (x86_64, aarch64)

6.7.1.2.5. FreeBSD
6.7.1.2.5.1. 12.1+ (amd64)
6.7.1.2.5.2. 13 (amd64)

6.7.1.2.6. Oracle Linux
6.7.1.2.6.1. 7.4+ (x86_64)
6.7.1.2.6.2. 8.1+ (x86_64, aarch64)

6.7.1.2.7. Red Hat Enterprise Linux (RHEL)
6.7.1.2.7.1. 7.4+ (x86_64, aarch64, ppc64le)
6.7.1.2.7.2. 8.1+ (x86_64, aarch64, s390x)

6.7.1.2.8. SUSE Linux Enterprise Server (SLES)
6.7.1.2.8.1. 12 SP5 (x86_64)
6.7.1.2.8.2. 15 SP2 (x86_64)

6.7.1.2.9. Ubuntu
6.7.1.2.9.1. 18.04 LTS (x86_64, aarch64)
6.7.1.2.9.2. 20.04 LTS (x86_64, aarch64, s390x)

6.7.1.3. Deve possuir ao menos um processo master e um processo worker
6.7.1.3.1. O processo master deve ser responsável pela leitura dos arquivos de configuração
6.7.1.3.2. O processo worker deve ser responsável pelo processamento das requisições
6.7.1.3.3. Deve ser possível configurar manualmente o número de processos worker
6.7.1.3.4. Deve ser possível ajustar automaticamente o número de processos worker com base na quantidade de CPU disponível

6.7.1.4. Quando a solução realizar cache devem existir processos específicos de cache loader e cache manager
6.7.1.5. Deve permitir aplicar as alterações na configuração sem interromper o processamento das requisições
6.7.1.6. Deve permitir a reconfiguração dinâmica do balanceamento dos servidores sem a necessidade de realizar reload da configuração
6.7.1.7. Deve possuir a capacidade de operar em alta disponibilidade nos modos ativo-ativo e ativo-standby
6.7.1.8. Deve suportar uso em alta disponibilidade com, pelo menos as seguintes funções:
6.7.1.8.1. Session caching: as sessões são compartilhadas entre os nodes
6.7.1.8.2. Resource limiting: cada node avalia os recursos locais e notifica os outros
6.7.1.8.3. Dynamic configuration: mudanças dinâmicas na configuração são compartilhadas entre os nodes

6.7.1.9. Deve realizar, pelo menos, os seguintes métodos de balanceamento do tráfego HTTP:
6.7.1.9.1. Round robin

6.7.1.9.2. Least connections
6.7.1.9.3. IP Hash
6.7.1.9.4. Generic Hash
6.7.1.9.5. Least time

6.7.1.10. Deve realizar, pelo menos, os seguintes métodos de balanceamento do tráfego TCP e UDP:
6.7.1.10.1. Round robin
6.7.1.10.2. Least connections
6.7.1.10.3. Hash
6.7.1.10.4. Least time

6.7.1.11. Deve ser capaz de configurar o tempo no qual as conexões para um servidor crescem gradativamente
6.7.1.12. Deve realizar o processamento de tráfego HTTP
6.7.1.13. Deve permitir a inclusão de dados na resposta dos servidores/aplicações
6.7.1.14. Deve ser capaz de realizar o processamento de requisições que terminem em "/"
6.7.1.15. Deve ser capaz de manipular a resposta do servidor e especificar o content-type
6.7.1.16. Deve ser capaz de gerar um gif com apenas um pixel
6.7.1.17. Deve ser capaz de retirar a compressão da resposta dos servidores para enviar aos clientes que não possuem suporte a GZIP
6.7.1.18. Deve ser capaz de realizar a compressão da resposta do servidor antes de enviar aos clientes
6.7.1.19. Deve ser capaz de adicionar campos na resposta do servidor antes de enviar para os clientes
6.7.1.20. Deve ser capaz de definir arquivos que serão utilizados no index
6.7.1.21. Deve ser capaz de tornar aleatória a escolha do arquivo de index
6.7.1.22. Deve ser capaz de alterar IP e porta do cliente para valores que estiverem no cabeçalho
6.7.1.23. Deve ser capaz de realizar filtragem de comandos nas respostas
6.7.1.24. Deve ser capaz de definição de cookies para identificação dos clientes
6.7.1.25. Deve ser capaz de gerenciamento de arquivos para facilitar a atualização dos websites utilizando WebDAV
6.7.1.26. Deve possuir suporte a Brotli como algoritmo para compressão de dados
6.7.1.27. Deve ser capaz de realizar a identificação da localização do cliente pelo IP, contendo: região, estado, cidade, ISP
6.7.1.28. Deve possuir suporte a Lua para manipulação de requisições MySQL, PostgreSQL, Memcached, Redis, e upstream HTTP web services
6.7.1.29. A solução deve, quando habilitado, permitir a proteção das aplicações através de WAF
6.7.1.30. A solução deve ter suporte ao uso de framework para rastreamento do cliente, compatível com Zipkin, Jaeger e Datadog
6.7.1.31. A solução deve ter suporte ao controle de acesso baseado em endereço IP (Access Control List - ACL)
6.7.1.32. A solução deve implementar autenticação HTTP Basic
6.7.1.33. A solução deve realizar validação de JSON Web Tokens
6.7.1.34. A solução deve realizar autorização de clientes através de requisições a um autenticador externo
6.7.1.35. A solução deve realizar controle de acesso através do campo Referer contido no cabeçalho HTTP
6.7.1.36. A solução deve realizar verificação de autenticidade através do tempo de expiração do link
6.7.1.37. A solução deve realizar a criação de variáveis baseado no valor do User-Agent contido no cabeçalho HTTP dos clientes
6.7.1.38. A solução deve dividir as requisições em sub-requisições e cada uma poderá ser respondida com cache
6.7.1.39. A solução deve permitir a criação de variáveis baseadas em outras variáveis
6.7.1.40. A solução deve permitir a alteração da URI solicitada ou realizar o redirect
6.7.1.41. A solução deve realizar segregação de tráfego baseado em variáveis (Teste A/B)
6.7.1.42. A solução deve realizar alteração de textos na resposta aos clientes
6.7.1.43. A solução deve logar transações HTTP local ou remotamente
6.7.1.44. A solução deve realizar a agregação de log das transações HTTP por sessão
6.7.1.45. Deve realizar proxy para, pelo menos, as seguintes tecnologias:
6.7.1.45.1. F4F: Stream HDS (Adobe HTTP Dynamic Streaming; filename extensions .f4f, .f4m, .f4x)
6.7.1.45.2. FLV: realizar Stream FLV (Flash Video; filename extension .flv)
6.7.1.45.3. HLS: realizar Stream HLS (Apple HTTP Live Streaming; filename extensions .m3u8, .ts) dinamicamente gerado de MP4 ou MOV (extensões .m4a, .m4v, .mov, .mp4, .qt)
6.7.1.45.4. MP4: realizar Stream MP4 (extensões .m4a, .m4v, .mp4)
6.7.1.45.5. FastCGI: realizar Proxy e cache das requisições para FastCGI server
6.7.1.45.6. gRPC: realizar Proxy das requisições para gRPC server
6.7.1.45.7. Memcached: realizar Proxy das requisições para memcached server
6.7.1.45.8. Mirror: enviar cópias das requisições para um ou mais servidores
6.7.1.45.9. Proxy: realizar Proxy e cache das requisições para HTTP server
6.7.1.45.10. SCGI: realizar Proxy e cache das requisições para SCGI server
6.7.1.45.11. Upstream: realizar Proxy e cache das requisições para servidores que estão sendo balanceados
6.7.1.45.12. Uwsgi: realizar Proxy e cache das requisições para uwsgi server

6.7.1.46. Deve suportar a monitoração dos servidores que estão sendo balanceados através, pelo menos, dos seguintes parâmetros:
6.7.1.46.1. Intervalo entre monitoração
6.7.1.46.2. Variação do tempo entre cada monitoração
6.7.1.46.3. Falhas consecutivas (quantidade de falhas para considerar o servidor "fora do ar")
6.7.1.46.4. Acertos consecutivos (quantidade de acertos para considerar o servidor "no ar")
6.7.1.46.5. URI
6.7.1.46.6. Porta
6.7.1.46.7. gRPC

6.7.1.47. Possuir recursos para balancear novas sessões, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
6.7.1.47.1. Por cookie: inserção de um novo cookie na sessão
6.7.1.47.2. Por cookie: utilização do valor do cookie da aplicação

6.7.1.48. Deve realizar controle de tráfego HTTP através de, pelo menos, os seguintes parâmetros:
6.7.1.48.1. Limitação de quantidade de conexões
6.7.1.48.2. Limitação de quantidade de requisições
6.7.1.48.3. Limitação de quantidade de respostas

6.7.1.49. Deve possuir suporte a HTTP/2

6.7.1.50. Deve suportar, pelo menos, os seguintes padrões de SSL/TLS:
6.7.1.50.1. SSLv2
6.7.1.50.2. SSLv3
6.7.1.50.3. TLSv1
6.7.1.50.4. TLSv1.1
6.7.1.50.5. TLSv1.2
6.7.1.50.6. TLSv1.3

6.7.1.51. Deve suportar a realização de proxy para protocolos de correio eletrônico:
6.7.1.51.1. IMAP
6.7.1.51.2. POP3
6.7.1.51.3. SMTP

6.7.1.52. Deve possibilitar a configuração através de REST API

6.7.1.53. Deve realizar o controle de acesso utilizando autenticação JWT

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

6.7.2 Ingress Controller

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

6.7.2.1.1 Kubernetes 1.24 – 1.19
6.7.2.1.2 NIC Helm Chart 0.14.0
6.7.2.1.2 NIC Operator 1.1.0

6.7.2.2 Deve estar disponível como Docker image em pelo menos:

6.7.2.2.1 Alpine 3.16
6.7.2.2.2 Debian bullseye-slim
6.7.2.2.3 Debian buster-slim
6.7.2.2.4 RedHat ubi8

6.7.2.3 Deve ser compatível com Kubernetes Ingress API v1

6.7.2.4 Deve realizar circuit breaking

6.7.2.5 Deve realizar distribuição blue-green

6.7.2.6 Deve realizar canary testing

6.7.2.7 Deve realizar A/B testing

6.7.2.8 Deve realizar routing

6.7.2.9 Deve realizar header manipulation

6.7.2.10 Deve realizar autenticação mTLS

6.7.2.11 Deve realizar WAF

6.7.2.12 Deve suportar WebSocket

6.7.2.13 Deve realizar reescrita de URL

6.7.2.14 Deve suportar HTTP/2

6.7.2.15 Deve ser compatível com Helm Charts

6.7.2.16 Deve realizar persistência de sessão

6.7.2.17 Deve realizar monitoração em tempo real

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

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

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

6.7.2.21 Deve disponibilizar estatísticas em tempo real do tráfego

6.7.2.22 Deve possuir integração nativa com Grafana e Prometheus

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

6.7.2.23.1 Accepted client connections
6.7.2.23.2 Active client connections
6.7.2.23.3 Dropped client connections
6.7.2.23.4 Total http requests
6.7.2.23.5 Current http requests
6.7.2.23.6 Successful SSL handshakes
6.7.2.23.7 Failed SSL handshakes
6.7.2.23.8 Session reusing during SSL handshakes
6.7.2.23.9 Client connections that are currently being processed
6.7.2.23.10 Total Connections
6.7.2.23.11 Total Sessions Completed
6.7.2.23.12 Connections completed without creating a session
6.7.2.23.13 Bytes received from clients
6.7.2.23.14 Bytes sent to clients

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

6.8. Serviços de Implantação e Configuração (Grupo 03)

6.8.1 Serviços de atualização e migração para o novo appliance

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

6.8.1.1.1 Instalar fisicamente o apliance no rack;

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

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

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

6.8.1.2.1 Versão TMOS e hotfixes instalados;

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

6.8.1.2.3 Perfis, políticas e objetos compartilhados;

6.8.1.2.4 Licenciamento atual (chave de ativação) e suporte;

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

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

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

6.8.1.2.8 Configurações de certificados, chaves, perfis SSL.

6.8.1.3 Validação de compatibilidade no momento da migração;

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

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

6.8.1.4 Elaborar plano de migração contendo:

6.8.1.4.1 Procedimento para rollback em cado de falha;

6.8.1.4.2 Testes de conectividade;

6.8.1.5 Migração das configurações:

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

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

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

6.8.1.6 Testes e Validações

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

6.8.1.6.2 Validar health monitors e status de pools/nodes;

6.8.1.6.3 Testar persistência, iRules, compressão, SSL offload;

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

6.8.1.6.5 Medir performance básica (latência, throughput);

6.8.1.7 Ativação em produção

6.8.1.7.1 Programar janela de mudança;

6.8.1.7.2 Trocar cabos/tráfego para o novo r5800;

6.8.1.7.3 Monitorar métricas e logs;

6.8.1.8 Pós-Migração

6.8.1.8.1 Registrar serial e ativar suporte no myF5;

6.8.1.8.2 Atualizar documentação de topologia e configurações;

6.8.1.8.3 Desativar o i5800 conforme planejamento realizado;

6.9 Serviços de implantação e Configuração para o Base Package:

6.9.1. HTTP Load Balancers

6.9.1.1 Será configurado um HTTP Load Balancer contendo até 15 FQDNs para atender às aplicações do ambiente, com as seguintes características, conforme necessário:
6.9.1.1.1 Domains and LB Type.
6.9.1.1.2 Custom TLS Certificate.
6.9.1.1.3 Routes.

6.9.2 Origin Pools

6.9.2.1 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.

6.9.2.2 Configuração de Health Check

6.9.3 Web Application Firewall (WAF)

6.9.3.1 Configuração da Política de Segurança
6.9.3.1.1 Será criada uma política de WAF para cada HTTP Load Balancer, com as seguintes características:

6.9.3.1.1.1 Attack Signatures: All Attack Types, High and Medium Signatures.
6.9.3.1.1.2 Automatic Attack Signatures Tuning.
6.9.3.1.1.3 Threat Campaigns.
6.9.3.1.1.4 Violations.
6.9.3.1.1.5 Signature-Based Bot Protection.

6.9.4.2 Operação
6.9.4.2.1 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.

6.9.5 DoS Protection

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

6.9.5.1.1 L7 DDoS Auto Mitigation;

6.9.5.1.2 Slow DDoS Mitigation.

6.9.6 Common Security Controls

6.9.6.1 Service Policies
6.9. 6.1.1 Serão configuradas até 5 service policies, que poderão ser replicadas para mais de um HTTP Load Balancer.

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

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

6.9.6.4 Global Log Receiver
6.9.6.4.1 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.

6.9.7 Serviços de Configuração para API Protection

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

6.9.7.1.1 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'.

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

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

6.9.8 Malicious Users

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

6.9.8.1.1 Configuração para identificação de usuários;

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

6.9.9 Serviços de Configuração para o Bot Defense

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

6.9.9.1.1 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.

6.9.10 Serviços de Configuração para o Web App Scan

6.9.10.1 Será realizada uma varredura automatizada do ambiente, por domínio, com o objetivo de identificar os serviços expostos e detectar possíveis problemas.
6.9.10.2 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.

6.10 Serviços de Configuração para o NGINX ONE por node

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

6.10.2 Descrição do Serviço

6.10.2.1 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.

6.10.2.2 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.

6.11 Serviços de Consultoria e Suporte Técnico

6.11.1 Serviços que não se aplicam a este grupo e já estão cobertos pela garantia do fabricante e que serão destacados no item 15:

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

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

6.11.1.3 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;

6.11.2 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.

6.11.3 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.

6.11.4 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.

6.11.5 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.

6.11.6 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.

6.11.7 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.

6.11.8 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.

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

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

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

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

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

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

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

6.11.11.1 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.

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

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

6.11.12.2 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.

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

6.11.13 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.

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

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

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

6.11.17 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.

6.11.18 O suporte remoto deverá contemplar, no mínimo:

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

6.11.18.2 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.

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

6.11.18.4 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.

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

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

6.11.19.2 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.

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

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

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

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

6.11.19.7 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.

6.11.19.8 Auxílio na auditoria e análise de "logs".

7. DA NECESSIDADE DE FORMALIZAÇÃO DE CONTRATO

7.1 Os eventuais acionamentos da ARP resultante do pregão ensejarão formalização de contrato para os serviços previstos neste Estudo Técnico Preliminar (ETP), tendo em vista as características do objeto a ser contratado, com a existência de obrigações futuras, incluindo a garantia, continuidade e confiabilidade do mesmo, com vigência de:

7.1.1 06 (seis) meses para a eventual renovação da garantia F5 BIG-IP i5800 Best Bundle (com IP Intelligence) suporte Premium 24x7;

7.1.2 36 (trinta e seis) meses para os licenciamentos e para a eventual atualização/substituição do appliance da solução i5800 para a linha r5800.

7.2 A duração desses contratos poderá ser prorrogada, desde que justificadamente, pelo prazo necessário à conclusão do objeto, conforme Art. 6º, XVII, da Lei Federal n.° 14.133/2021.

8. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

8.1. Tendo por objetivo assegurar a proteção contínua das aplicações críticas do Tribunal de Justiça do Estado do Amazonas (TJAM), garantir a alta disponibilidade dos serviços judiciais e administrativos, fortalecer a segurança cibernética e atender às exigências normativas vigentes, estima-se contratar:

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

9. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

9.1 Os valores estimados para esta contratação seguem na planilha abaixo.

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$ 529.188,00	R$ 529.188,00
	2	Atualização/substituição do appliance da solução i5800 para a linha r5800 pelo período de 36 meses	02	02	unidade	R$ 423.035,00	R$ 846.070,00
	3	Licenciamento Best Bundle (com IP Intelligence) e suporte Premium 24x7 pelo período de 36 (trinta e seis) meses	02	02	unidade	R$ 1.447.831,50	R$ 2.895.663,00
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$ 681.878,60	R$ 681.878,60
	5	Licença F5 NGINX ONE por instância com suporte Premium 24x7 pelo período de 36 (trinta e seis) meses	01	01	unidade	R$ 150.531,30	R$ 150.531,30
	6	Licença F5 NGINX ONE por node com suporte Premium 24x7 pelo período de 36 (trinta e seis) meses	01	04	unidade	R$ 34.371,00	R$ 137.484,00
03	**Serviços de Implantação**						

7	Serviço de migração e atualização linha “i” 5800 para “r”5800	01	01	unidade	R$ 172.500,00	R$ 172.500,00
8	Serviço de implantação da solução Base Package (item 4)	01	01	unidade	R$ 63.500,00	R$ 63.500,00
9	Serviço de implantação da solução NGINX ONE (item 05 e/ou 06)	01	01	unidade	R$ 58.850,00	R$ 58.850,00
10	Serviços de Consultoria e/ou Suporte Técnico (banco de horas)	100	500	hora	R$ 590,00	R$ 295.000,00
VALOR TOTAL ESTIMADO DO SRP					**R$ 5.830.664,90**	

10. JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

10.1 O objeto da contratação possui características comuns e usuais, fornecido por várias empresas, porém deverá ser realizada por único fornecedor. O parcelamento do objeto, neste caso, é inviável já que não se justifica técnica e economicamente, além do que a solução de TI contratada é composta de serviços integrados e correlatos que visam manter em funcionamento toda infraestrutura de solução.

11. CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

11.1 Não há contratações correlatas.

12. RESULTADOS PRETENDIDOS

12.1 Economicidade, eficácia, eficiência: com esta pretensa contratação, busca-se preservar os investimentos realizados no ambiente do TJAM, mantendo-se a eficácia, integração e a qualidade da plataforma de segurança em um ambiente de TI complexo como o do TJAM, bem como reduzir possíveis impactos gerados pela indisponibilidade dos serviços e sistemas de TIC e também evitar a reimplementação das barreiras de seguranças já em operação do TJAM;

12.2. Melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis: com a efetivação da contratação, o CONTRATANTE poderá direcionar seus esforços na capacitação da equipe técnica da SETIC para matérias mais relevantes, estratégicas e alinhadas com o negócio do TJAM, já que durante o período de vigência dos equipamentos o corpo técnico da SETIC adquiriu amplo conhecimento e experiência na solução de segurança atual;

12.3. Impactos ambientais positivos: não se aplica;

12.4. Melhoria da qualidade de produtos ou serviços oferecidos à sociedade: com a efetivação da contratação, a tendência esperada é a de menos ataques cibernéticos, reduzindo-se assim potenciais indisponibilidades nos serviços oferecidos à sociedade.

13. PROVIDÊNCIAS PARA ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO

13.1 Não haverá necessidade de adequação de ambiente.

14. IMPACTOS AMBIENTAIS

14.1 Aplicar, no que couber, a Resolução CNJ nº 400 de 16 de junho de 2021 que dispõe sobre a política de sustentabilidade no âmbito do Poder Judiciário.

15. SERVIÇOS DE MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

15.1. 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.

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

15.2.1. 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.

15.2.2. 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.

15.2.3. 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.

16. DECLARAÇÃO DE VIABILIDADE (OU NÃO) DA CONTRATAÇÃO

16.1 Considerando todo o exposto acima, esta Secretaria de Tecnologia da Informação e Comunicação declara que a renovação do licenciamento e a expansão da Solução de Segurança F5 BIG-IP Best Bundle, com a inclusão dos módulos Distributed Cloud e NGINX, é fundamental e viável, diante da necessidade de assegurar a continuidade da proteção das aplicações críticas do TJAM, elevar o nível de resiliência cibernética institucional e fortalecer a infraestrutura tecnológica frente aos desafios atuais de segurança da informação.

16.2 A contratação é imprescindível para manter a alta disponibilidade dos serviços judiciais e administrativos, garantir a integridade e a confidencialidade dos dados institucionais, proteger aplicações e APIs expostas à Internet e cumprir as diretrizes normativas estabelecidas na Resolução CNJ nº 468/2022, Resolução CNJ nº 396/2021, Resolução CNJ nº 370/2021 e na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

16.3 Destaca-se que a solução atualmente implantada no Tribunal já desempenha papel estratégico na proteção contra-ataques cibernéticos, na gestão segura de acessos e na otimização do tráfego de rede, sendo a continuidade e a ampliação da solução fundamentais para garantir a estabilidade, a eficiência e a segurança dos serviços prestados pelo TJAM à sociedade.

17. OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS

17.1 A contratada deverá garantir as melhores práticas relacionadas à Segurança da Informação e à Lei Geral de Proteção de Dados Pessoais (LGPD), principalmente, no que diz respeito aos dados pessoais tratados durante a configuração dos privilégios.

17.2 A contratada durante a execução do objeto, deve implementar medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados.

17.3 Será exigido da Contratada que cada profissional que venha a prestar serviços assine um termo de compromisso, pelo qual se comprometerá a manter o sigilo das informações.

17.4 A Contratada deverá manter sigilo absoluto a respeito de quaisquer dados, informações e artefatos, contidos em documentos e mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos, independentemente da classificação de sigilo conferido pelo TJAM a tais documentos.

18. MAPEAMENTO DE RISCOS

FASE: ESTUDO TÉCNICO PRELIMINAR												
ID	**CAUSA (DEVIDO A)**	**EVENTO (PODERÁ OCORRER)**	**CONSEQUÊNCIA (O QUE PODERÁ LEVAR A)**	**PROB.**	**IMPACTO**	**NÍVEL**	**RESPOSTA**	**MEDIDAS PREVENTIVAS (PARA EVITAR QUE OCORRA)**	**MEDIDAS DE CONTINGÊNCIA (SE OCORRER, O QUE DEVE SER FEITO)**	**RESPONSÁVEL**	**PRAZO**	**MONITORAMENTO**
R1	Falta de alinhamento entre a necessidade e o escopo técnico do ETP	Elaboração de requisitos técnicos incompletos ou divergentes	Atrasos na contratação e necessidade de revisão do ETP	3	4	Alto	Revisar constantemente os requisitos	Reuniões de alinhamento entre a SETIC e as unidades demandantes	Ajustar rapidamente os requisitos técnicos	SETIC	Durante a elaboração do ETP	Acompanhamento das atas de reunião e validações
R2	Subestimação dos custos e da abrangência da solução	Estimativas de valores abaixo dos preços praticados no mercado	Restrição orçamentária e necessidade de revisão do estudo técnico	2	4	Moderado	Revisão detalhada das estimativas de custo	Pesquisa de preços de mercado atualizada e ampla	Readequar o escopo e as estimativas orçamentárias	SETIC	Durante a elaboração do ETP	Revisão contínua das informações de mercado
R3	Incompleta identificação das necessidades institucionais	Definição inadequada do objeto da contratação	Necessidade de reabertura do processo ou revisão do ETP	1	4	Baixo	Revisão da descrição das necessidades	Consulta ampla às áreas usuárias e análise do planejamento estratégico	Ajustar o objeto da contratação antes da conclusão do ETP	SETIC	Durante a elaboração do ETP	Validação da necessidade com os gestores
R4	Não renovação do licenciamento da solução F5 BIG-IP	Interrupção dos serviços de proteção	Risco à integridade, disponibilidade e	3	5	Alto	Informar à alta gestão	Monitorar a vigência do licenciamento e	Renovar o licenciamento com	SETIC	Durante a vigência do	Acompanhamento do ciclo de vida da licença

		do ambiente tecnológico do TJAM	confidencialidade dos dados judiciais					planejar renovação com antecedência	prioridade, antes do vencimento		contrato atual	
R5	Não contratação ou renovação da solução WAF F5 BIG-IP	Indisponibilidade dos recursos de Load Balance, persistência de cookies e sessões	Indisponibilidade parcial ou total do sistema judicial PROJUDI, afetando a prestação jurisdicional	3	5	Alto	Garantir a contratação/renovação do WAF F5 com antecedência	Estabelecer cronograma de renovação com prazos definidos e revisões periódicas do contrato	Ativar ambiente de contingência ou infraestrutura alternativa em caso de falha do WAF	SETIC	Durante a vigência do contrato atual	Acompanhamento contínuo da vigência contratual
R6	Não contratação da expansão para F5 Distributed Cloud e NGINX	Falta de proteção adequada para APIs e aplicações em nuvem	Fragilidade da segurança, risco de ataques e baixa resiliência do ambiente moderno	3	5	Alto	Informar à alta gestão	Justificar tecnicamente a expansão com base na Resolução CNJ nº 370/2021	Priorizar a contratação da expansão conforme demanda tecnológica	SETIC	Durante o planejamento do TR	Monitoramento do volume de APIs e arquitetura de aplicações

NÍVEL DE RISCO

Alto: Obrigatoriedade de tratamento do risco por meio de ação, monitoramento, e controle efetivo.

Moderado: Recomendável o tratamento do risco por meio de ação, monitoramento, e controle.

Baixo: Não há obrigatoriedade de tratamento do risco, cabendo uma reavaliação no ciclo posterior e/ou decisão da alta direção do TJAM quanto à emissão de ação, após a análise do tema em questão.

Baixo	Menor e/ou igual a 5.
Moderado	Entre 6 e 9.
Alto	Maior que 9.

IMPACTO			
	5	15	25
	3	9	15
	1	3	5
	PROBABILIDADE		

Manaus, data registrada no sistema.

Washington Alves da Cunha Neto	**Diogo Mendonça de Sousa**	**Breno Figueiredo Corado**
Assessor de Segurança da Informação e Proteção de Dados	Diretor da Divisão de Infraestrutura de Tecnologia da Informação e Comunicação	Secretário de Tecnologia da Informação e Comunicação
Assinado Digitalmente	Assinado Digitalmente	Assinado Digitalmente

Documento assinado eletronicamente por **DIOGO MENDONCA DE SOUSA**, **Diretor(a)**, em 12/09/2025, às 12:30, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **WASHINGTON NETO**, **Coordenador(a)**, em 12/09/2025, às 12:30, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BRENO FIGUEIREDO CORADO**, **Secretário(a)**, em 12/09/2025, às 13:39, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2436772** e o código CRC **D990702B**.