



EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO
Gerência de Segurança da Informação
Rua Líbero Badaró, 425, - Bairro Centro - São Paulo/SP - CEP 01009-905
Telefone: 3396-9000

Termo de Referência

PROCESSO Nº 7010.2026/0005768-5

TERMO DE REFERÊNCIA

**CONTRATAÇÃO DE SOLUÇÃO DE PROTEÇÃO DE APLICAÇÕES WEB E APIS
(CLOUD WAF/WAAP)**

DIRETORIA DE INFRAESTRUTURA E TECNOLOGIA

Julho / 2026

1. OBJETO

Contratação de **solução de proteção de aplicações web e APIs (Cloud WAF/WAAP)**, fornecida exclusivamente como serviço em nuvem (**Cloud Native/SaaS**), incluindo licenciamento por subscrição, implantação, configuração, suporte técnico, manutenção, treinamento e serviços especializados.

Não serão aceitas soluções baseadas em *appliances* físicos, *appliances* virtuais, máquinas virtuais, *containers* ou quaisquer componentes instalados ou hospedados nos datacenters da CONTRATANTE, ainda que operem de forma integrada com serviços em nuvem.

A solução deverá atender integralmente aos requisitos técnicos, funcionais, operacionais, de segurança da informação, privacidade e conformidade legal definidos neste Termo de Referência.

1.1. Tabela de Composição dos Itens

Item	Descrição	Unidade	Quantidade
1	Serviço WAF/WAAP em Nuvem (SaaS)	UN	01
2	Subscrições de Softwares e Licenças	UN	01
3	Implantação e Configuração completa da solução WAF/WAAP, contemplando todos os serviços e componentes em nuvem fornecidos pela CONTRATADA, incluindo integração com o ambiente da CONTRATANTE, parametrização inicial, operação assistida inicial e validação funcional de todos os requisitos previstos neste Termo de Referência.	UN	01
4	Suporte Técnico, Manutenção e Garantia	Anual	03
5	Treinamento (06 vagas de treinamento, distribuídas em no mínimo 3 turmas)	UN	06
6	Pacotes de Licenciamento por Aplicações (FQDN) ou Throughput (Mbps ou Gbps) ¹	Blocos de 100	07
7	Consultoria Técnica Especializada (sob demanda) (consultoria para tuning, novas implementações e mudanças de arquitetura)	Pacotes de 100 Horas	03

1 Modelo de licenciamento (FQDN x Throughput) e equivalência técnica

Será admitido modelo de licenciamento baseado em throughput, quantidade de aplicações (FQDN), ou combinação de ambos, desde que atendidas as seguintes condições:

- Quando adotado licenciamento por throughput, a licitante deverá informar, de forma clara, o volume de tráfego suportado, bem como o número máximo de aplicações, domínios e APIs protegidos simultaneamente pelo pacote ofertado;
- Quando adotado licenciamento por aplicação (FQDN), deverão ser explicitados, por aplicação, os limites máximos de throughput, requisições por segundo (RPS) e conexões simultâneas;
- Independentemente do modelo, a licitante deverá apresentar, juntamente com a proposta técnica, tabela de equivalência de capacidade, demonstrando de forma clara e objetiva que a solução ofertada atende simultaneamente ao ambiente estimado de referência, contemplando, no mínimo:
 - número máximo de aplicações (FQDNs) protegidas simultaneamente;
 - throughput médio e de pico suportados;
 - limitações de requisições por segundo (RPS), conexões simultâneas e sessões TLS.

Parágrafo único: Não serão aceitas soluções cujo atendimento aos parâmetros acima seja alternativo ou mutuamente excludente, devendo todos os limites declarados serem suportados de forma simultânea.

Ambiente Estimado de Referência

Para fins de comparação técnica e econômica entre as propostas, considera-se como **ambiente estimado mínimo de referência**:

- 700 (setecentas) aplicações web e/ou APIs (FQDNs)** protegidas simultaneamente;
- Throughput médio sustentado mínimo de 1,5 Gbps**, considerando tráfego HTTPS com inspeção SSL/TLS ativa;
- Throughput máximo (pico) mínimo de 2 Gbps** com inspeção SSL/TLS ativa;
- Taxa média de 10.000 (dez mil) requisições por segundo (RPS)**, com picos de até **30.000 RPS**;
- Predominância de **tráfego de APIs REST e JSON**, estimado em no mínimo **30% do volume total**.

Os parâmetros definidos neste ambiente estimado de referência representam valores para fins de dimensionamento técnico e comparação entre propostas, não significando que todos ocorrerão simultaneamente e de forma sustentada em regime permanente.

A licitante deverá dimensionar sua solução de forma proporcional e tecnicamente justificável, considerando variações de tráfego, perfis de uso e picos eventuais.

A solução ofertada deverá atender integralmente a esse ambiente estimado durante toda a vigência contratual, sem degradação de desempenho.

A CONTRATANTE poderá avaliar a equivalência técnica e econômica entre propostas com diferentes modelos de licenciamento, com base nas informações apresentadas e na documentação oficial do fabricante.

Para fins de julgamento das propostas, a capacidade mínima considerada equivalente será o atendimento simultâneo de:

- 700 FQDNs protegidos;
- Throughput sustentado de 1,5 Gbps;
- Throughput de pico de 2 Gbps;
- 30.000 requisições por segundo (RPS).

A proposta será considerada habilitada somente quando atender todos os parâmetros acima de forma simultânea, independentemente do modelo comercial adotado pelo fabricante.

2. VIGÊNCIA

O contrato terá vigência de 36 (trinta e seis) meses, contados da data de sua assinatura, podendo ser prorrogado conforme a legislação vigente, em especial a Lei Federal nº 13.303/2016.

O período de suporte técnico, manutenção, garantia, subscrições e demais serviços recorrentes terá início a partir da emissão do Termo de Aceite dos Serviços de Implantação e Configuração e permanecerá vigente pelo prazo de 36 (trinta e seis) meses.

Os prazos de entrega, implantação, configuração, treinamentos e demais obrigações contratuais previstas neste Termo de Referência serão contados a partir da assinatura do contrato.

3. CONTEXTO E JUSTIFICATIVA

A contratação tem por objetivo reforçar a proteção das aplicações web e APIs da Administração Municipal, mitigando riscos associados a:

- Ataques previstos no **OWASP Top 10 Web e OWASP Top 10 API**;
- Ataques de negação de serviço (DDoS);
- Bots maliciosos e automações abusivas;
- Exploração de vulnerabilidades conhecidas ou desconhecidas.

Busca-se, ainda, padronizar a camada de segurança de aplicações, garantir alta disponibilidade dos serviços prestados ao cidadão, aumentar a observabilidade e atender integralmente às exigências legais, em especial a **Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018)**.

4. ANÁLISE DE RISCOS, PRIVACIDADE E LGPD

Como condição para o aceite da solução, a CONTRATADA deverá apresentar:

- Documento de Análise de Riscos da Solução WAF/WAAP, contemplando riscos à confidencialidade, integridade, disponibilidade e privacidade;

- b) Mapeamento dos fluxos de dados inspecionados, processados ou armazenados, inclusive em componentes em nuvem;
- c) Medidas técnicas e administrativas de mitigação.

Quando houver tratamento de dados pessoais, a CONTRATADA deverá fornecer todas as informações técnicas necessárias para subsidiar a elaboração ou atualização do Relatório de Impacto à Proteção de Dados Pessoais (RIPD/DPIA) pela CONTRATANTE, conforme art. 38 da Lei nº 13.709/2018 (LGPD).

A aprovação desses documentos é condição para o **aceite definitivo da solução**.

5. REQUISITOS TÉCNICOS DA SOLUÇÃO

5.1. Arquitetura

· A solução deverá operar exclusivamente em arquitetura em nuvem (Cloud/SaaS), provida pelo fabricante ou parceiro autorizado, sem utilização de *appliances* físicos ou virtuais instalados nos datacenters da CONTRATANTE, devendo assegurar equivalência funcional, operacional e de segurança.

5.1.1. Compatibilidade com Ambiente Existente

- A solução ofertada deverá ser compatível e interoperável com o ambiente atual da CONTRATANTE, que contempla a utilização de balanceadores de carga baseados em plataforma F5 BIG-IP i10600, versão 15.1.10.3 ou superior.
- A compatibilidade deverá abranger, no mínimo:
 - a) funcionamento integrado em arquiteturas com balanceadores existentes, incluindo cenários em camada L4 e/ou L7;
 - b) preservação de funcionalidades de balanceamento, roteamento e alta disponibilidade já implementadas;
 - c) interoperabilidade com mecanismos de encaminhamento de tráfego, terminação SSL/TLS e políticas de segurança existentes;
 - d) ausência de dependência obrigatória de substituição integral da infraestrutura atualmente em operação.
- A CONTRATADA deverá apresentar, no momento da proposta técnica ou durante a fase de aceite, documentação técnica oficial ou evidências que comprovem a compatibilidade e o correto funcionamento da solução no ambiente descrito.
- A eventual necessidade de ajustes, integrações ou adaptações para garantir essa compatibilidade deverá estar contemplada no escopo da contratação, sem ônus adicional à CONTRATANTE.
- Em arquiteturas híbridas ou em nuvem, será admitida a utilização de ambientes do fabricante para funcionalidades como:

5.1.2. Mitigação de ataques DDoS volumétricos

- Capacidade comprovada de mitigação de ataques de negação de serviço (DDoS), contemplando:
 - a) Ataques volumétricos em camadas L3 e L4, por meio de mecanismos dedicados, próprios ou de parceiros tecnológicos do fabricante, com capacidade mínima sustentada de mitigação equivalente a, no mínimo, 5 vezes o throughput máximo estimado do ambiente de referência, ou capacidade superior sob demanda, desde que contratualmente garantida e tecnicamente comprovada;
 - b) Ataques em camada L7 (HTTP/HTTPS), incluindo floods de requisições, ataques de exaustão de sessão e ataques combinados;
 - c) Capacidade de mitigação sustentada por tempo contínuo, sem limitação artificial de duração;
 - d) A mitigação volumétrica deverá ocorrer na infraestrutura global de nuvem da solução ofertada;
 - e) Para esses casos, deverá ser apresentada documentação técnica que comprove as capacidades de mitigação volumétrica, os fluxos de tráfego envolvidos e as garantias de conformidade com a LGPD;
 - f) Documentação técnica oficial do fabricante que comprove as capacidades informadas.

5.1.3. Inteligência contra bots e automações

A solução WAF/WAAP deverá possuir capacidades avançadas de detecção, classificação e mitigação de bots e tráfego automatizado, utilizando técnicas modernas de análise comportamental, fingerprinting e inteligência adaptativa, atendendo aos seguintes requisitos:

- 5.1.3.1. Identificação e Classificação de Bots. A solução deverá ser capaz de identificar e classificar diferentes tipos de bots, incluindo, mas não limitado a:
 - a) Bots maliciosos (scrapers, credential stuffing, carding, scalping, account takeover).
 - b) Bots automatizados distribuídos (botnets).
 - c) Bots legítimos (motores de busca, crawlers autorizados).
 - d) Deve realizar distinção precisa entre usuários humanos e automação, minimizando impactos em usuários legítimos.
- 5.1.3.2. Análise Comportamental e Fingerprinting
 - a) Implementação de mecanismos avançados de fingerprinting de dispositivos (ex.: browser, sistema operacional, padrões de execução JavaScript).
 - b) Capacidade de análise comportamental em tempo real, incluindo:
 - c) Padrões de navegação e interação.
 - d) Velocidade e frequência de requisições.
 - e) Movimentos e eventos (quando aplicável).
 - f) Suporte à identificação de bots sofisticados que utilizam técnicas de evasão (ex.: headless browsers, spoofing, rotação de IP).
- 5.1.3.3. Detecção de Automação Avançada
 - a) Capacidade de detectar ataques automatizados como:
 - b) Credential stuffing e brute force distribuído.
 - c) Scraping massivo de dados.
 - d) Criação automatizada de contas falsas.
 - e) Uso de modelos dinâmicos (incluindo IA/ML, quando aplicável) para identificação de padrões não previamente conhecidos.

5.1.3.4. Abuso de APIs

- a) A solução deverá detectar e mitigar API Abuse (OWASP API Security Top 10), implementando proteção contra:
 - BOLA (Broken Object Level Authorization);
 - Broken Authentication;
 - Exposição excessiva ou abusiva de dados;
 - Mass Assignment;
 - API Business Logic Abuse;
 - Shadow APIs;
 - Zombie APIs.
- b) A solução deverá suportar inspeção e proteção nativa para APIs GraphQL, incluindo limitação de profundidade de consultas, introspection e proteção contra abuso de queries;
- c) A solução deverá suportar inspeção e proteção de APIs baseadas em gRPC.

5.1.3.5. Mitigação Inteligente de Bots

- a) A solução deverá suportar múltiplos mecanismos de mitigação, tais como:
- b) Bloqueio seletivo de bots maliciosos.
- c) Rate limiting adaptativo baseado em comportamento.
- d) Desafios progressivos (CAPTCHA, JavaScript challenges, proof-of-work).
- e) Degradação controlada de resposta (tarpitting).
- f) Aplicação de políticas diferenciadas conforme classificação do bot (allow, monitor, challenge, block).

5.1.4. Análise comportamental e correlação de eventos

- A solução poderá processar tráfego, payloads, metadados e eventos de segurança em sua infraestrutura global, desde que observados os requisitos da LGPD, criptografia, controle de acesso, rastreabilidade e retenção definidos pela CONTRATANTE.
- Quando houver transferência internacional de dados, metadados ou eventos de segurança, a CONTRATADA deverá comprovar a adoção dos mecanismos previstos nos arts. 33 a 36 da Lei nº 13.709/2018 (LGPD), incluindo cláusulas contratuais, certificações, normas corporativas globais ou mecanismos equivalentes legalmente admitidos.
- Será admitida, mediante justificativa técnica e documental, a utilização de ambientes do fabricante para o processamento temporário e transitório de metadados técnicos, eventos de segurança, informações estatísticas ou dados anonimizados, desde que:
 - a) não contenham dados pessoais identificáveis, payloads completos ou informações sensíveis;
 - b) estejam protegidos por criptografia forte em trânsito e em repouso;
 - c) observem a legislação vigente, em especial a LGPD;
 - d) tenham localização e prazos de retenção previamente informados e aprovados pela CONTRATANTE;
 - e) possam ser eliminados integralmente ao término do contrato ou mediante solicitação formal da CONTRATANTE.
- Quando a solução envolver componentes em nuvem, CDN ou serviços gerenciados do fabricante, a CONTRATADA deverá **informar de forma clara e documentada**:
 - a) as **localizações geográficas (regiões/PoPs)** utilizadas para processamento ou inspeção de tráfego;
 - b) os **fluxos de dados envolvidos**, indicando se há processamento de metadados, eventos de segurança ou informações estatísticas fora dos ambientes da CONTRATANTE;
 - c) os **prazos de retenção aplicáveis**.
- O fornecimento dessas informações não implica autorização automática para tratamento de dados fora dos ambientes da CONTRATANTE, permanecendo aplicáveis todas as restrições estabelecidas neste Termo de Referência e na legislação vigente.

5.2. Desempenho, Capacidade e Escalabilidade

- A solução WAF/WAAP deverá ser dimensionada para operação em **ambientes críticos de grande porte**, garantindo, no mínimo:
 - a) **Throughput HTTPS mínimo garantido**, considerando inspeção SSL/TLS ativa, compatível com TLS 1.2 e TLS 1.3, conforme documentação técnica oficial do fabricante;
 - b) Capacidade mínima de processamento simultâneo de conexões e requisições HTTP/HTTPS em camadas L4 e L7, compatível com ambientes de missão crítica;
 - c) Processamento criptográfico realizado integralmente pela solução, sem degradação significativa de desempenho, mesmo com inspeção profunda de payloads, APIs REST e JSON;
 - d) Capacidade de mitigação de ataques volumétricos e de exaustão de recursos, incluindo ataques de negação de serviço em camadas L3, L4 e L7.
 - e) A solução não deverá introduzir latência adicional superior a 10 ms (dez milissegundos) por requisição (ou pelo valor definido no plano de homologação), em condições normais de operação, considerando tráfego com inspeção ativa de SSL/TLS;
 - f) A solução deverá possuir mecanismos de identificação de acessos automatizados, incluindo bots avançados, agentes autônomos e automações baseadas em inteligência artificial, quando suportados pelo fabricante, permitindo a aplicação de políticas de monitoramento, limitação ou bloqueio conforme o perfil identificado.
- A comprovação das capacidades acima deverá ser realizada por meio de **documentação técnica oficial do fabricante**, tais como datasheets, white papers ou relatórios técnicos equivalentes.
- A solução deverá permitir **crescimento escalável**, vertical e/ou horizontal, sem a necessidade de substituição integral dos componentes originalmente contratados, devendo suportar ampliação de capacidade mediante adição de licenças, subscrições ou instâncias adicionais.

5.3. Preservação do IP de Origem

- A solução deverá garantir que o backend das aplicações receba o **endereço IP original do cliente final**, operando como serviço cloud proxy ou CDN.
- Serão aceitos mecanismos padronizados como:
 - a) X-Forwarded-For (XFF);
 - b) True-Client-IP;

- c) Ou método equivalente oficialmente suportado.
- Deverá existir mecanismo de **validação contra spoofing**.
- A CONTRATADA deverá entregar, no aceite, **documentação de arquitetura** detalhando o fluxo de IP de origem.

5.3.1. Bloqueio por IP de Origem em Cenários sem Preservação do IP

- A solução deverá permitir a implementação de políticas de bloqueio e controle de acesso baseadas em endereço IP de origem por aplicação (FQDN), mesmo em cenários onde o IP real do cliente final não esteja diretamente disponível para a aplicação protegida.
- Para esses casos, a solução deverá oferecer mecanismos alternativos que possibilitem a identificação e o controle do IP de origem, tais como:
 - a) utilização de metadados, headers HTTP ou informações de sessão inseridas ou tratadas pela própria solução;
 - b) associação de conexões, sessões ou outros atributos técnicos que permitam a identificação inequívoca da origem do acesso;
 - c) mecanismos equivalentes oficialmente suportados pelo fabricante.
- A configuração dessas políticas deverá ser realizada de forma simples, intuitiva e independente de customizações complexas na aplicação, incluindo alterações de código ou dependências específicas de componentes como arquivos WEB.CONFIG.
- Esse requisito aplica-se especialmente a aplicações legadas ou que implementam controle de acesso diretamente na camada de aplicação (ex.: via configuração de servidor web), devendo a solução possibilitar a centralização dessas políticas na camada de segurança WAF/WAAP.
- A CONTRATADA deverá comprovar, por meio de documentação técnica ou evidências práticas durante a fase de aceite, a viabilidade e o correto funcionamento desses mecanismos no controle de acesso por IP em nível de aplicação.
- A solução deverá implementar e suportar **proteção de Sessão**:
 - d) Session Hijacking;
 - e) Session Fixation;
 - f) Cookie Tampering;
 - g) Token Replay.

5.4. Crescimento e Garantia de Capacidade

- A solução deverá permitir expansão de capacidade mediante contratação adicional de licenças, subscrições ou recursos equivalentes, sem necessidade de substituição integral da arquitetura originalmente implantada e sem interrupção relevante dos serviços protegidos.
- A ampliação de capacidade deverá ocorrer, quando necessária, exclusivamente por meio da adição de licenças, subscrições ou instâncias adicionais, conforme modelo suportado pelo fabricante.

5.5. Funcionalidades de Proteção de Aplicações Web e APIs (WAAP)

- A solução deverá oferecer, no mínimo, as seguintes funcionalidades, **com comprovação documental e operacional**:
 - a) Descoberta de APIs expostas, inclusive APIs não documentadas, por meio de análise automática de tráfego em tempo de execução e/ou mecanismos assistidos ou semi-automáticos, baseados em correlação de chamadas, logs ou integração com gateways e repositórios de definição de APIs, desde que devidamente documentados e operacionalmente comprovados durante a fase de aceite técnico;
 - b) Validação de schemas de APIs, suportando padrões OpenAPI/Swagger;
 - c) Criação e aplicação de políticas de segurança por endpoint e método HTTP;
 - d) Mecanismos de rate limiting e controle de burst por IP, aplicação ou endpoint;
 - e) Virtual patching para mitigação de vulnerabilidades conhecidas e emergentes;
 - f) Cobertura integral contra ataques descritos no OWASP Top 10 – Web e OWASP Top 10 – API;
 - g) Detecção e mitigação de bots maliciosos e automações abusivas, com diferenciação entre tráfego legítimo e automatizado.
- Durante a fase de aceite técnico, a CONTRATADA poderá ser demandada a apresentar **evidências funcionais**, tais como relatórios, telas de configuração ou testes práticos, que comprovem o atendimento aos requisitos acima.

5.6. Operação, Observabilidade e Integração

- A solução deverá possuir integração nativa com sistemas SIEM/SOAR, suportando, no mínimo:
 - a) Envio de eventos por syslog, CEF, LEEF ou APIs;
 - b) Inclusão obrigatória dos seguintes campos nos eventos: IP de origem real do cliente, método HTTP, URI ou endpoint, ação tomada, regra acionada, severidade e timestamp;
 - c) Envio de eventos em tempo próximo ao real (near real time);
 - d) Integração sem necessidade de desenvolvimento customizado oneroso.
- A solução deverá possuir também:
 - e) Métricas operacionais (RPS, latência, códigos HTTP, eventos de segurança);
 - f) Automação via APIs e integração com CI/CD e IaC;
 - g) Geração de relatórios técnicos e executivos.

5.7. Logs, Auditoria e Retenção

- A solução deverá permitir:
 - a) Retenção mínima de 90 dias de logs de segurança e eventos operacionais em ambiente seguro disponibilizado pela solução cloud ou integrado ao SIEM da CONTRATANTE;
 - b) A retenção mínima de logs poderá ser implementada por meio de:

- armazenamento nativo da própria solução;
- dispositivos ou storages externos homologados; ou
- infraestrutura de armazenamento sob controle da CONTRATANTE, desde que garantida a integridade, a confidencialidade e a disponibilidade das informações.
- Parágrafo único: Os custos necessários ao cumprimento do prazo mínimo de retenção deverão estar incluídos na proposta comercial, não sendo admitida cobrança adicional posterior.
- c) Exportação integral de logs para sistemas externos de SIEM/SOAR, sem custo adicional;
- d) Diferenciação entre logs operacionais, logs de segurança e logs de APIs;
- e) Geração de logs específicos para APIs contendo, no mínimo, metadados de requisição, endpoint, método HTTP, código de resposta e ação aplicada, vedado o armazenamento de payloads completos contendo dados pessoais sensíveis.

5.8. Alta Disponibilidade (HA) e Continuidade Operacional

- A solução deverá operar em arquitetura de alta disponibilidade, suportando, no mínimo:
 - a) Topologia ativo/ativo ou ativo/passivo, devidamente descrita na documentação de arquitetura;
 - b) Failover automático entre os nós da solução, sem intervenção manual, garantindo tempo máximo de indisponibilidade compatível com a arquitetura técnica adotada pela solução, comprovado por meio de testes em ambiente da CONTRATANTE durante a fase de aceite técnico;
 - c) Para arquiteturas distribuídas baseadas em CDN, Anycast, DNS Global Load Balancing ou tecnologia equivalente, será aceito tempo de convergência compatível com a arquitetura apresentada, desde que devidamente justificado e documentado;
 - d) Tempo de interrupção compatível com ambientes críticos, devidamente documentado;
 - e) Sincronização de políticas, configurações e estados de sessão entre os nós.
- Como condição para o aceite, a CONTRATADA deverá realizar teste de failover em ambiente da CONTRATANTE, comprovando o correto funcionamento do mecanismo de alta disponibilidade.

5.9. Administração Segura

- A solução deverá oferecer, no mínimo:
 - a) MFA e RBAC;
 - b) SSO (SAML ou OIDC);
 - c) Trilhas de auditoria e controle de alterações;
 - d) Registros auditáveis de acessos, alterações e eventos.

6. CONSULTORIA TÉCNICA ESPECIALIZADA

As horas do item “Consultoria Técnica Especializada” serão utilizadas sob demanda, mediante solicitação e aprovação da CONTRATANTE via Ordem de Serviço, para execução de atividades como:

- 6.1. ajustes finos (tuning) da solução;
- 6.2. implementação de novas aplicações ou APIs;
- 6.3. criação e revisão de políticas de segurança;
- 6.4. mudanças de arquitetura ou topologia;
- 6.5. apoio técnico em incidentes complexos;
- 6.6. evolução contínua da solução.

7. SEGURANÇA DO FABRICANTE E DA CADEIA DE SUPRIMENTOS

A CONTRATADA deverá comprovar que o fabricante da solução WAF/WAAP adota boas práticas de segurança no ciclo de vida de desenvolvimento de software, incluindo, no mínimo:

- 7.1. política formal de gerenciamento e divulgação responsável de vulnerabilidades;
- 7.2. O processo de correção de falhas e vulnerabilidades deverá observar política formal do fabricante baseada em análise de risco e criticidade, com compromisso de transparência quanto à classificação, comunicação e aplicação das correções, durante toda a vigência contratual.;
- 7.3. disponibilização de atualizações de segurança regulares durante toda a vigência contratual;
- 7.4. controles de segurança para proteção do código-fonte e da cadeia de desenvolvimento.

A CONTRATANTE poderá, a seu critério, solicitar evidências documentais dessas práticas, tais como declarações do fabricante, políticas públicas, certificações ou documentação técnica.

Caso a solução utilize componentes de terceiros ou software de código aberto, a CONTRATADA deverá assegurar que tais componentes sejam atualizados, suportados e livres de vulnerabilidades críticas conhecidas.

Para comprovação das boas práticas de segurança do fabricante, deverão ser apresentada as seguintes evidências documentais:

- a) Política pública de gerenciamento e divulgação responsável de vulnerabilidades;
- b) Base pública de CVEs ou advisories de segurança do fabricante;
- c) Certificação reconhecida de segurança da informação (ex.: ISO/IEC 27001, ISO/IEC 27701, SOC 2 Type II ou equivalente).

8. SUPORTE TÉCNICO E MANUTENÇÃO

Os serviços de suporte técnico, manutenção e garantia deverão ser prestados em regime **24 (vinte e quatro) horas por dia, 7 (sete) dias por semana**, durante toda a vigência contratual, abrangendo todos os componentes da solução WAF/WAAP.

A abertura de chamados poderá ser realizada por meio de portal, telefone, e-mail ou outro meio oficialmente disponibilizado pela CONTRATADA.

A CONTRATADA deverá garantir atendimento ininterrupto para chamados classificados como Severidade Alta (S1) ou Média (S2), **vedada a interrupção do atendimento antes da solução definitiva**, ainda que o atendimento se estenda para períodos

noturnos, finais de semana ou feriados, salvo autorização formal da CONTRATANTE.

A utilização de infraestrutura de terceiros, provedores de nuvem, CDNs ou serviços do fabricante **não exime a CONTRATADA da responsabilidade integral** pelo atendimento, suporte e manutenção da solução.

9. ACORDO DE NÍVEL DE SERVIÇO (SLA)

9.1. Classificação de Severidade

Os chamados de suporte deverão ser classificados conforme os seguintes níveis, definidos a critério da equipe técnica da CONTRATANTE:

- a) **Severidade Alta (S1) - Incidente Crítico**
Aplica-se a indisponibilidade total da solução WAF/WAAP, falhas que impeçam a proteção do tráfego de aplicações críticas, impossibilidade de gestão da solução ou incidentes de segurança com risco imediato à confidencialidade, integridade ou disponibilidade.
- b) **Severidade Média (S2) - Incidente Relevante**
Aplica-se à indisponibilidade parcial da solução, falhas em funcionalidades relevantes ou degradação significativa de desempenho.
- c) **Severidade Baixa (S3) - Incidente Não Crítico**
Aplica-se a falhas pontuais, dúvidas operacionais, ajustes de configuração ou problemas sem impacto relevante.

Chamados classificados como Severidade Baixa (S3) não serão abertos aos sábados, domingos e feriados, salvo autorização expressa da CONTRATANTE.

9.2. Tempos Máximos de Atendimento

Severidade	Início do Atendimento	Prazo Máximo para Solução Contorno	Prazo Máximo para Solução Definitiva
Alta (S1)	até 1 (uma) hora	até 4 (quatro) horas corridas	Plano de ação: até 8 (oito) horas. Solução definitiva: conforme criticidade e cronograma formal acordado entre as partes.
Média (S2)	até 1 (uma) hora	até 6 (seis) horas corridas	até 12 (doze) horas corridas
Baixa (S3)	até 4 (quatro) horas úteis	até 9 (nove) horas úteis	até 24 (vinte e quatro) horas úteis

9.3. Disponibilidade da Solução

A solução WAF/WAAP deverá garantir disponibilidade mínima mensal de 99,95% (noventa e nove vírgula noventa e cinco por cento), considerando todos os seus componentes críticos.

Para fins de cálculo de disponibilidade:

- Serão desconsideradas janelas de manutenção previamente acordadas entre as partes;
- Serão considerados eventos de indisponibilidade total ou parcial que impactem efetivamente a proteção ou o encaminhamento do tráfego das aplicações.

A CONTRATADA deverá disponibilizar relatórios mensais de disponibilidade, contendo o registro detalhado dos eventos de indisponibilidade, suas causas e tempos de resolução.

10. PENALIDADES, GLOSAS E NÍVEIS DE SERVIÇO (SLA)

10.1. Glosas de Pagamento (Descumprimento de SLA)

As glosas referem-se a descontos aplicados diretamente sobre o faturamento mensal da CONTRATADA, em decorrência do não atendimento dos níveis de serviço (SLA), não se caracterizando como sanção administrativa formal.

As glosas serão aplicadas automaticamente no faturamento do período correspondente ao descumprimento verificado, independentemente de processo administrativo sancionador.

10.1.1. Atraso no Início do Atendimento

Caso haja atraso no início do atendimento dos chamados, serão aplicadas glosas conforme abaixo:

- a) **0,1% por hora de atraso**, calculada sobre o valor mensal do serviço de suporte técnico do contrato, para qualquer nível de severidade.

10.1.2. Atraso na Solução de Contorno ou Definitiva

Serão aplicadas glosas progressivas conforme a severidade:

Severidade Alta (S1): 2% por hora de atraso, calculada sobre o valor mensal do serviço de suporte técnico do contrato;

Severidade Média (S2): 1% por hora de atraso, calculada sobre o valor mensal do serviço de suporte técnico do contrato;

Severidade Baixa (S3): 0,5% por hora útil de atraso, calculada sobre o valor mensal do serviço de suporte técnico do contrato.

10.1.3. Limite de Glosas

O somatório das glosas aplicadas em um mesmo período de faturamento poderá atingir até:

100% (cem por cento) do valor mensal do serviço afetado, nos casos de descumprimento relevante, indisponibilidade ou reincidência.

10.1.4. Reincidência

Caracteriza-se reincidência a ocorrência de:

3 (três) ou mais descumprimentos de SLA da mesma severidade, dentro do período de 12 (doze) meses.

Nesses casos, poderá ser aplicada, adicionalmente:

- a) glosa complementar de até **20% sobre o valor mensal do serviço afetado**; e/ou
- b) abertura de procedimento administrativo para avaliação de falha contratual grave.

10.2. Multas Contratuais (Sanção Administrativa)

As multas possuem natureza sancionatória e serão aplicadas mediante **procedimento administrativo formal**, assegurados o contraditório e a ampla defesa, nos termos da legislação vigente.

As multas aplicam-se a descumprimentos contratuais de natureza **não diretamente vinculada ao SLA operacional**, incluindo:

- a) atraso na implantação e configuração da solução;
- b) atraso na entrega de serviço cloud, instâncias, ativos ou licenças;
- c) atraso no início dos treinamentos;
- d) atraso na emissão de certificados de conclusão;
- e) descumprimento de obrigações contratuais relevantes.

10.2.1. Multas por Atrasos Contratuais

Aplicam-se as seguintes multas:

- a) **1% (um por cento) por dia de atraso** na implantação e configuração da solução, calculado sobre o valor do serviço correspondente;
- b) **0,2% (zero vírgula dois por cento) por dia de atraso** na entrega de serviço cloud, ativos ou licenças, calculado sobre o valor do item em atraso;
- c) **1% (um por cento) por mês de atraso** no início dos treinamentos, calculado sobre o valor total do item de treinamento;
- d) **0,5% (zero vírgula cinco por cento)** sobre o valor do item de treinamento, em caso de atraso na emissão de certificados.

10.3. Não Cumulatividade

Para um mesmo evento gerador:

- a) não haverá aplicação cumulativa entre glosa e multa;
- b) será aplicada a medida mais gravosa, conforme análise da CONTRATANTE.

10.4. Disposições Gerais

- a) As glosas incidirão diretamente no faturamento mensal;
- b) As multas dependerão de processo administrativo específico;
- c) Eventuais penalidades deverão ser interpretadas de forma sistemática, prevalecendo a regra mais específica;
- d) A aplicação das penalidades observará integralmente a legislação vigente.

11. SERVIÇO DE IMPLANTAÇÃO E CONFIGURAÇÃO

11.1. Serviço de Implantação e Configuração de Toda a Solução

11.1.1. Toda a solução objeto deste contrato, deverá estar configurada e em operação no prazo máximo de 30 dias corridos após a disponibilização das licenças.

11.2. Plano de Trabalho

11.2.1. No intuito de definir procedimentos para o bom andamento das atividades relacionadas neste termo de referência, será realizada, em até 5 dias úteis após a assinatura do contrato, uma reunião entre a CONTRATANTE e a CONTRATADA, para definição do plano de trabalho, que deverá conter, no mínimo, as seguintes etapas:

- 11.2.1.1. Implantação;
- 11.2.1.2. Planejamento e configuração da solução;
- 11.2.1.3. Testes e homologação;
- 11.2.1.4. A implantação da solução deverá contemplar:
 - 11.2.1.4.1. Testes de funcionalidades antes da entrada em produção;

- 11.2.1.4.2. Fase de validação em ambiente controlado (piloto);
- 11.2.1.4.3. Procedimento documentado de rollback;
- 11.2.1.4.4. Plano de contingência.
- 11.2.2. O plano de trabalho deverá conter, adicionalmente:
 - 11.2.2.1. Desenho topológico detalhado da solução (situação atual e proposta);
 - 11.2.2.2. Identificação dos pontos de inserção do WAF/WAAP na arquitetura existente;
 - 11.2.2.3. Análise de impacto na infraestrutura da CONTRATANTE;
 - 11.2.2.4. Definição de janelas de implantação, incluindo eventuais paradas programadas;
 - 11.2.2.5. Plano de rollback em caso de falha na implantação.
- 11.2.3. Neste documento estarão definidas as fases de entrega, implantação e configuração acordados entre a CONTRATANTE e a CONTRATADA.

11.3. Documentação Técnica

Deverão ser fornecidos juntamente com os produtos e licenças os manuais técnicos de referência, contendo todas as informações sobre os produtos com as instruções para configuração e operação, preferencialmente em português (Brasil), ou, na inexistência de tradução em português, podem ser escritos em Língua Inglesa.

12. TREINAMENTO

- 12.1. Os treinamentos deverão ser realizados e concluídos para até 6 (seis) funcionários da PRODAM, divididos em, no mínimo, 3 (três) turmas separadas, ambas dentro de prazo máximo de 180 (cento e oitenta) dias corridos, a contar da data de assinatura do contrato, de acordo com cronograma estabelecido entre a Equipe Técnica da PRODAM e a CONTRATADA, e deverão ser ministrados por instrutores preparados e certificados pelo fabricante do produto, com infraestrutura de hardware, software, laboratório de testes e material didático, — cumprindo o programa oficial de treinamento do fabricante, inclusive com aulas práticas e teóricas;
- 12.2. O prazo para agendamento dos treinamentos poderá ser ampliado mediante acordo entre as partes;
- 12.3. O cronograma para realização dos treinamentos deverá ser proposto pela CONTRATADA, em prazo máximo de 20 (vinte) dias corridos, contados da assinatura do contrato. A PRODAM analisará o cronograma, estabelecendo posteriormente, em até 5 (cinco) dias úteis, as datas definitivas com a CONTRATADA;
- 12.4. Serão aceitos vouchers para treinamentos em turmas abertas, desde que sejam realizadas por instrutores preparados e certificados pelo fabricante dos produtos, em centros de treinamento certificados pelo fabricante — com infraestrutura de hardware, software, laboratório de testes e material didático — cumprindo o programa oficial de treinamento do fabricante, inclusive com aulas práticas e teóricas;
- 12.5. A carga horária mínima deverá ser de 40 horas (ou período estipulado como treinamento oficial do fabricante constante em lista de venda para os itens adquiridos) e deverá abranger todas as facilidades da solução fornecida, cobrindo conteúdo teórico e prático, em nível avançado para a solução fornecida, incluindo tópicos e cenários avançados de arquitetura, implantação, configuração, operação e resolução de problemas;
- 12.6. Após a conclusão, a CONTRATADA deverá emitir o certificado de conclusão do treinamento;
- 12.7. Caso os treinamentos sejam realizados fora da cidade de São Paulo, despesas com transporte (aéreo e local), hospedagem e alimentação deverão ser custeadas pela CONTRATADA.
- 12.8. Em acordo entre as partes, poderão ser aceitos treinamentos “online”.
- 12.9. Os treinamentos deverão ser ministrados na língua portuguesa.

13. OBRIGAÇÕES DA CONTRATADA

- 13.1. A CONTRATADA deve cumprir todas as obrigações constantes neste Termo de Referência, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:
- 13.2. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas para atendimento aos requisitos descritos neste Termo de Referência e em sua proposta;
- 13.3. Reparar ou substituir, às suas expensas, quaisquer componentes físicos, virtuais ou lógicos da solução WAF/WAAP que apresentem falhas, defeitos ou não conformidades, conforme os prazos definidos neste Termo de Referência e de acordo com a severidade do incidente;
- 13.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a CONTRATANTE autorizada a descontar da garantia, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos;
- 13.5. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;
- 13.6. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à CONTRATANTE;
- 13.7. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços;
- 13.8. Prestar todo esclarecimento ou informação solicitada pela CONTRATANTE ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução dos serviços;
- 13.9. Paralisar, por determinação da CONTRATANTE, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;
- 13.10. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do contrato;
- 13.11. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado;
- 13.12. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina;
- 13.13. Submeter previamente, por escrito, à CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo;
- 13.14. Não permitir a utilização de qualquer trabalho do menor de dezoito anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;
- 13.15. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de

- habilitação e qualificação exigidas na licitação;
- 13.16. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;
- 13.17. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da CONTRATANTE;
- 13.18. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;
- 13.19. Durante toda a vigência contratual, a CONTRATADA deverá assegurar, sem ônus adicional:
- 13.19.1. atualizações de software, firmware, bases de segurança e assinaturas;
- 13.19.2. correções de falhas, bugs e vulnerabilidades identificadas;
- 13.19.3. atualização ou substituição de componentes descontinuados;
- 13.19.4. compatibilidade contínua entre os componentes da solução;
- 13.19.5. acesso irrestrito às áreas de suporte técnico e documentação oficial do fabricante.
- 13.20. As obrigações acima aplicam-se a todos os componentes da solução, independentemente de serem executadas diretamente pela CONTRATADA ou pelo fabricante, permanecendo a CONTRATADA integralmente responsável pelo cumprimento contratual.
- 13.21. Executar a integração de todos os produtos da solução, de modo a não prejudicar as atividades mantidas nos locais, podendo ser exigida a realização de algumas fases em horários noturnos e fins de semana para que seja cumprido o cronograma de entrega da CONTRATANTE;
- 13.21.1. Providenciar o planejamento de testes, fornecendo um “Plano de Homologação e Testes” contendo todo o processo de homologação dos produtos e detalhamento dos testes que serão executados para validar a solução implementada;
- 13.21.2. Executar uma série de testes funcionais básicos para verificar o perfeito funcionamento do ambiente, seguindo os procedimentos definidos no “Plano de Homologação e Testes”, sendo tais testes a serem obrigatoriamente executados nos componentes de hardware e software envolvidos no projeto;
- 13.21.3. Elaborar a “Documentação e Finalização do Projeto”, que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e ou gerencial.
- 13.22. Durante a implantação da solução, a CONTRATADA deverá realizar, entre outras atividades: análise de performance, *tuning*, resolução de problemas e implantação e ajustes de controles de segurança.
- 13.23. Caberá à CONTRATADA a disponibilização de todos os recursos necessários, tais como hardwares, softwares e recursos humanos necessários à implantação da solução.
- 13.24. A CONTRATADA realizará adequação/configuração da solução fornecida ao longo da etapa de migração e realização de novas configurações.
- 13.25. A CONTRATADA deverá manter registro detalhado de todas as atividades executadas durante a vigência contratual, incluindo:
- 13.25.1. Atendimentos realizados;
- 13.25.2. Alterações de configuração;
- 13.25.3. Intervenções na solução;
- 13.25.4. Utilização de horas técnicas;
- 13.25.5. Registros de incidentes e respectivos tratamentos;
- 13.25.6. Tais registros deverão ser disponibilizados à CONTRATANTE sempre que solicitado.

13.26. Transição e Encerramento Contratual

Ao término da vigência contratual, ou em caso de rescisão, a CONTRATADA deverá:

- a) Garantir a exportação integral das configurações, políticas de segurança, registros e logs gerados pela solução;
- b) Fornecer documentação atualizada da arquitetura e configurações implementadas;
- c) Realizar transferência de conhecimento para a equipe técnica da CONTRATANTE;
- d) Remover acessos, credenciais e quaisquer vínculos ativos com os ambientes da CONTRATANTE;
- e) Assegurar a eliminação segura de quaisquer dados sob sua responsabilidade que estejam fora do ambiente da CONTRATANTE.

As atividades de transição deverão ser realizadas sem impacto à continuidade operacional dos serviços.

14. OBRIGAÇÕES DA CONTRATANTE

- 14.1. Prover acesso a rede física ou lógica sob demanda;
- 14.2. Ajustes na rede lógica da Prodam quando necessário;
- 14.3. Prover informações do ambiente de infraestrutura da Prodam para colaborar na solução de problemas;
- 14.4. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;
- 14.5. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;
- 14.6. As funções de gestão e fiscalização do contrato não recairão sobre o mesmo servidor, com as atribuições conforme a seguir especificadas:
- 14.6.1. Fiscal do Contrato: agirá de forma ativa e preventiva, observando o cumprimento, pela CONTRATADA, de todas as regras previstas contratualmente, além de buscar os resultados esperados do pacto com redução efetiva das inconsistências nos procedimentos de sua execução e, ainda, registrar todas as ocorrências relacionadas com a execução do contrato e encaminhar informações ao gestor do contrato.
- 14.6.2. Gestor do Contrato: irá controlar o processo referente ao contrato, zelando para que constem todos os documentos relativos à contratação, tais como: termo de referência/projeto básico, termo de contrato, ordem de serviço, portarias de nomeação/alteração de fiscal do contrato sempre que ocorrerem termos aditivos, termos de apostilamento, documentos fiscais, liquidações, obrigatoriedade de retenção na fonte dos tributos, entre outros.
- 14.7. Notificar a CONTRATADA por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;
- 14.8. Pagar à CONTRATADA o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;
- 14.9. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da CONTRATADA, no que couber;
- 14.10. Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;
- 14.11. Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;
- 14.12. Arquivar, entre outros documentos, projetos, as built, especificações técnicas, orçamentos, termos de recebimento,

contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas.

15. VISITA TÉCNICA

- 15.1. Com a finalidade de propiciar às LICITANTES o pleno conhecimento das condições e informações necessárias à adequada elaboração das propostas e à correta execução dos serviços, será facultada a realização de visita técnica para conhecimento do ambiente de infraestrutura em uso na PRODAM.
- 15.2. O prazo para realização da visita técnica iniciar-se-á no primeiro dia útil subsequente à publicação do Edital, estendendo-se até o terceiro dia útil anterior à data prevista para a abertura da sessão pública.
- 15.3. A visita técnica poderá ser realizada nas modalidades presencial ou remota, por meio de ferramenta de reuniões online disponibilizada pela PRODAM, a critério da LICITANTE e mediante agendamento prévio.
- 15.4. Para agendamento e realização da visita, o LICITANTE, ou seu representante legal, deverá estar devidamente identificado, mediante apresentação de documento de identidade oficial com foto e de documento expedido pela empresa que comprove sua autorização para representá-la na realização da visita técnica.
- 15.5. O agendamento deverá ser efetuado de segunda a sexta-feira, no horário das 08h00 às 12h00 e das 13h30 às 17h00, por meio do endereço eletrônico: <seinfo@prodam.sp.gov.br>, devendo ser indicada, no ato da solicitação, a modalidade de visita pretendida (presencial ou remota).
- 15.6. No caso de visita técnica remota, a PRODAM disponibilizará o acesso à reunião virtual, bem como as orientações necessárias para conexão, sendo responsabilidade da LICITANTE garantir a infraestrutura tecnológica adequada para participação.
- 15.7. Por ocasião da visita técnica, seja presencial ou remota, acompanhada por representante(s) do corpo técnico da PRODAM, a LICITANTE deverá apresentar a Declaração de Visita Técnica (ANEXO VII) devidamente preenchida, a qual será assinada, ao término da visita, por, no mínimo, 1 (um) membro do corpo técnico da PRODAM, com a devida comprovação da realização.
- 15.8. O LICITANTE que optar pela não realização da visita técnica declara-se plenamente ciente de que a vistoria foi facultada, assumindo integralmente os riscos e as consequências decorrentes do eventual desconhecimento das condições, ambiente e infraestrutura envolvidos na execução do objeto.

16. CONFIDENCIALIDADE

- 16.1. A CONTRATADA deverá zelar pelo sigilo de quaisquer informações referentes à estrutura, sistemas, usuários, contribuintes, topologia, e ao modo de funcionamento e tratamento das informações da CONTRATANTE, durante e após fim do contrato, salvo se houver autorização expressa da CONTRATANTE para divulgação;
- 16.2. Não haverá nenhum tipo de facilidade de acesso remoto, tão menos envio de forma automática ou controlada de informações (backdoor) originadas de software/hardware contratado ou adquirido sem o conhecimento e formal autorização da CONTRATANTE. A não observância desse fato poderá ser considerada espionagem e será motivo de processo civil e criminal conforme legislação vigente.

17. TRATAMENTO, RETENÇÃO E SOBERANIA DOS DADOS

Quando a solução envolver componentes em nuvem do fabricante, a CONTRATADA deverá informar de forma clara e documentada:

- a) a localização dos ambientes onde ocorrerá o processamento ou armazenamento de logs, metadados e eventos de segurança;
- b) os prazos de retenção dos logs e informações coletadas;
- c) os mecanismos de eliminação segura dos dados, ao término do contrato ou mediante solicitação da CONTRATANTE.

É vedado o uso, compartilhamento ou retenção de dados da CONTRATANTE para fins distintos da execução do objeto contratual. Os dados coletados pela solução deverão permanecer sob controle da CONTRATANTE, respeitando integralmente os princípios da LGPD e da legislação vigente.

Os ambientes utilizados para armazenamento persistente de logs, metadados e eventos de segurança deverão estar localizados no Brasil ou em países com nível adequado de proteção de dados reconhecido pela legislação brasileira, observados os requisitos da LGPD.

18. QUALIFICAÇÃO TÉCNICA

- 18.1. A licitante deverá apresentar Atestado(s) de Capacidade Técnica, emitido(s) em papel timbrado por pessoa jurídica de direito público ou privado, que comprove(m) experiência comprovada na implantação, operação e suporte de soluções WAF/WAAP SaaS ou Cloud-Native, compatíveis com o objeto desta contratação.
 - 18.1.1. Para eventuais esclarecimentos, caso seja necessário durante a licitação, o(s) atestado(s) deverá(ão):
 - a) **Estar devidamente datado(s) e assinado(s);**
 - b) Conter **identificação clara do atestante** (nome, cargo e empresa/instituição, telefone, e-mail etc.);
 - c) Ser (em) emitido(s) por pessoa jurídica CONTRATANTE dos serviços prestados.
 - 18.1.2. Será aceita a apresentação de um único atestado ou a somatória de mais de um, desde que, em conjunto, comprovem a execução de serviços pertinentes, compatíveis com o objeto da contratação;
- 18.2. Caso o licitante não seja o fabricante da solução ofertada, deverá apresentar comprovação de que a LICITANTE possui autorização do fabricante para comercializar, instalar e prestar suporte no Brasil para o produto especificado. A comprovação deverá ser feita por meio de Declaração do fabricante dos produtos que compõem a solução e destinada a PRODAM e com referência explícita a este processo licitatório.
- 18.3. A licitante deverá apresentar, juntamente com sua proposta comercial: catálogos, folder, manuais e demais documentos técnicos que comprovem a aderência da solução às especificações técnicas mínimas a serem indicadas no termo de referência.
- 18.4. Para fins de verificação de adequação da solução ofertada as especificações técnicas detalhadas apresentadas neste Termo de Referência deverão ser comprovadas em uma Matriz ponto-a-ponto contendo, de forma organizada, o item do Termo de Referência, o nome do arquivo da documentação original do fabricante e a indicação do número da página que comprove o atendimento ao item.
- 18.5. Para fins de julgamento das propostas a equipe de apoio técnico realizará a conferência técnica dos documentos exigidos, a saber:
 - 18.5.1. Os atestados de capacidade técnica apresentados pelos licitantes estão em compatibilidade com os serviços ou fornecimentos realizados com o objeto licitado, conforme especificado no Termo de Referência;
 - 18.5.2. A Declaração emitida pelo Fabricante comprova que a licitante está autorizada a comercializar, instalar e prestar suporte no Brasil para o produto especificado;
 - 18.5.3. Marca e modelo dos equipamentos ofertados, para verificação de sua aderência às especificações técnicas constantes do Termo de Referência;

- 18.5.4. Acessórios complementares, quando indicados, para confirmação de sua necessidade e compatibilidade com a solução proposta;
- 18.5.5. Catálogos, folder, manuais e demais documentos técnicos, juntamente com a Matriz Ponto-a-Ponto que será confrontada, com os requisitos mínimos exigidos, considerando aspectos como desempenho, capacidade, compatibilidade, certificações e demais parâmetros definidos neste Termo de Referência;
- 18.5.6. A verificação será conduzida por equipe de apoio técnico designada, com base nos critérios objetivos descritos na seção Requisitos Técnicos da Solução.
- 18.5.7. Toda comprovação documental exigida neste Termo de Referência deverá ser consolidada em uma única Matriz de Conformidade Técnica (Matriz Ponto-a-Ponto), contendo:
- a) requisito do TR;
 - b) descrição do atendimento;
 - c) referência do documento do fabricante;
 - d) nome do documento;
 - e) página correspondente;
 - f) observações complementares.
- 18.5.8. A ausência da comprovação poderá ensejar diligência ou desclassificação da proposta.

19. ACEITE

- 19.1. O aceite provisório contemplará ativação da plataforma, provisionamento das licenças e disponibilização do ambiente cloud. O aceite definitivo se dará após a conclusão da configuração, integração, migração das aplicações, testes de homologação e validação operacional.
- 19.2. O aceite das Licenças será formalizado pela CONTRATANTE mediante a emissão do Termo de Aceite e Recebimento das Licenças, no prazo de até 5 (cinco) dias úteis após a entrega do pacote de licenças, juntamente com a implantação e configuração da solução objeto deste edital.
- 19.3. O aceite do Serviço de Implantação e Configuração será formalizado mediante a emissão do Termo de Aceite dos Serviços de Implantação e Configuração no prazo de até 5 (cinco) dias úteis após a finalização da implantação e configuração completa da solução, desde que confirmada a conformidade com todos os requisitos estabelecidos neste Termo de Referência.
- 19.3.1. O aceite dos serviços de implantação e configuração estará condicionado à comprovação, pela CONTRATADA, do pleno funcionamento da solução, mediante execução de testes técnicos incluindo, no mínimo:
- 19.3.1.1. Bloqueio efetivo de ataques previstos no OWASP Top 10 – Web e API;
 - 19.3.1.2. Preservação e entrega do endereço IP real do cliente final ao backend da aplicação;
 - 19.3.1.3. Funcionamento do mecanismo de alta disponibilidade, com testes de failover automático;
 - 19.3.1.4. Inspeção e validação de tráfego HTTPS, incluindo APIs REST, com validação de schema quando aplicável;
 - 19.3.1.5. Integração funcional com solução de SIEM/SOAR da CONTRATANTE, com envio de logs e eventos;
 - 19.3.1.6. Aplicação de políticas de rate limiting, proteção contra bots e ataques automatizados;
 - 19.3.1.7. Os testes poderão ser realizados mediante scripts OWASP, ferramentas de mercado ou simulações controladas, com evidências documentais (prints, logs ou relatórios);
 - 19.3.1.8. Para fins de comprovação do atendimento aos testes técnicos exigidos, serão aceitas como evidência, isoladas ou combinadas:
 - a) Capturas de tela (prints) das interfaces administrativas da solução;
 - b) Logs exportados ou relatórios técnicos gerados automaticamente;
 - c) Relatórios de testes realizados com ferramentas reconhecidas de mercado;
 - d) Demonstração assistida da funcionalidade, mediante solicitação da CONTRATANTE.
 - 19.3.1.9. A não conformidade em qualquer dos testes poderá ensejar ajustes, correções e nova homologação, sem ônus adicional para a CONTRATANTE.
- 19.3.2. Entende-se pela implantação e configuração a disponibilização de todas as funcionalidades exigidas neste Termo de Referência e devidamente identificadas pela solução de gerenciamento.
- 19.4. O aceite de Treinamento ocorrerá após a finalização dos treinamentos. A CONTRATANTE emitirá o “Termo de Aceite de Recebimento do Treinamento” em até 5 (cinco) dias úteis após a formalização pela CONTRATADA da finalização do processo de treinamento e confirmação que todos os quesitos foram cumpridos conforme esse Termo de Referência.
- 19.4.1. Caso o treinamento fornecido não esteja de acordo com o que foi especificado, o Termo de Aceite de Recebimento do Treinamento não será emitido, devendo a CONTRATADA fornecer novo treinamento que contemple todos os requisitos necessários;
- 19.4.2. A CONTRATADA deverá emitir “Certificado de Conclusão”, em até 15 dias úteis após o término do treinamento;
- 19.4.3. Caso o certificado de conclusão do treinamento fornecido não seja emitido de acordo com o que foi especificado, o Termo de Aceite de Recebimento do Treinamento não será emitido, devendo a CONTRATADA providenciar sua emissão.
- 19.5. O Termo de Aceite de Recebimento das Licenças possui caráter de recebimento provisório dos respectivos componentes fornecidos, ficando o faturamento condicionado à emissão do Termo de Aceite dos Serviços de Implantação e Configuração da Solução Cloud WAF/WAAP.
- 19.6. O recebimento definitivo da solução ocorrerá somente após a conclusão da implantação, configuração, integração, testes e homologação, mediante emissão do Termo de Aceite dos Serviços de Implantação e Configuração, que comprovará o atendimento integral dos requisitos estabelecidos neste Termo de Referência.
- 19.7. Em razão da natureza integrada da solução WAF/WAAP, a disponibilização das licenças ou a ativação das subscrições não caracterizam, isoladamente, a conclusão do objeto contratado.
- 19.8. O início do faturamento dos itens recorrentes da solução, bem como a contagem do período de suporte, manutenção, garantia e subscrições, ficará condicionado à emissão do Termo de Aceite dos Serviços de Implantação e Configuração, que caracteriza o recebimento definitivo e a entrada da solução em operação.

20. CONDIÇÕES DE FATURAMENTO

- 20.1. O valor dos itens 1, 2, 4 e 6 da Tabela de Composição de Itens será faturado mensalmente em parcelas iguais, durante toda a vigência contratual, a partir da emissão do “Termo de Aceite dos Serviços de Implantação e Configuração” (Anexo III);
- 20.2. O valor do item 3 (implantação e configuração completa) da Tabela de Composição de Itens será faturado em parcela única, após a emissão do “Termo de Aceite dos Serviços de Implantação e Configuração” (Anexo III);
- 20.3. O valor do item 5 (Treinamento) da Tabela de Composição de Itens será faturado integralmente após a conclusão e aceite da última turma prevista, a partir da emissão do “Termo de Aceite e Recebimento do Treinamento” (Anexo V);
- 20.4. O valor do item 7 (Consultoria) da Tabela de Composição de Itens será faturado sob demanda e em parcela única, após a emissão do “Termo de Aceite da Ordem de Serviço de Consultoria” (Anexo VIII).

21. CONDIÇÕES DE PAGAMENTO

- 21.1. A Nota Fiscal Eletrônica de Serviços deverá ser emitida e encaminhada à CONTRATANTE, através do setor de Expediente, por meio do endereço eletrônico gfl@prodam.sp.gov.br
- 21.2. Após o recebimento da Nota Fiscal Eletrônica de Serviços, a CONTRATANTE disporá de até 05 (cinco) dias úteis para emissão do Termo de Aceite de Pagamento, aprovando os serviços prestados.
- 21.3. O pagamento será realizado por intermédio de crédito em conta corrente ou por outra modalidade que possa vir a ser determinada pela Gerência de Planejamento e Controle Financeiro (GFP), em 40 (quarenta) dias corridos a contar da data de emissão do Termo de Aceite de Pagamento.
- 21.4. Caso a Nota Fiscal Eletrônica de Serviços contenha divergências com relação ao estabelecido no Instrumento Contratual, a CONTRATANTE ficará obrigada a comunicar a empresa CONTRATADA, formalmente, o motivo da não aprovação no prazo de 05 (cinco) dias úteis. A devolução da Nota Fiscal Eletrônica de Serviços, devidamente, regularizada pela CONTRATADA, deverá ser efetuada em até 05 (cinco) dias úteis da data de comunicação formal realizada pela CONTRATANTE.
- 21.5. Em caso de atraso de pagamento dos valores devidos à CONTRATADA, mediante requerimento formalizado por esta, incidirão juros moratórios calculados utilizando-se o índice oficial de remuneração básica de caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança, para fins de compensação da mora (TR + 0,5% “pro rata tempore”), observando-se para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorreu.

São Paulo, 16 de julho de 2026.

WAGNER KANAGUSUKO
Gerente de Segurança da Informação - GIT

ANEXO I - PROPOSTA COMERCIAL

PE nº /202_

Declaramos que esta proposta tem validade pelo prazo de 60 dias, contados da data de abertura desta proposta, e que concordamos com todas as condições estabelecidas neste edital e seus respectivos anexos.

Item	Descrição	Unidade	Quantidade	Valor Unitário R\$	Valor Total R\$
1	Serviço WAF/WAAP em Nuvem (SaaS)	UN	01		
2	Subscrições de Softwares e Licenças	UN	01		
3	Implantação e Configuração completa da solução WAF/WAAP, contemplando todos os serviços e componentes em nuvem fornecidos pela CONTRATADA, incluindo integração com o ambiente da CONTRATANTE, parametrização inicial, operação assistida inicial e validação funcional de todos os requisitos previstos neste Termo de Referência.	UN	01		
4	Suporte Técnico, Manutenção e Garantia	Anual	03		
5	Treinamento (06 vagas de treinamento, distribuídas em no mínimo 3 turmas)	UN	06		
6	Pacotes de Licenciamento por Aplicações (FQDN) ou Throughput (Mbps ou Gbps) ¹	Blocos de 100	07		
7	Consultoria Técnica Especializada (sob demanda) (consultoria para tuning, novas implementações e mudanças de arquitetura)	Pacotes de 100 Horas	03		

Preço Total (postado no sistema) por extenso.

A CONTRATADA deverá apresentar seus preços com todos os impostos, encargos e taxas inclusos nos preços.

Local e Data
NOME / RAZÃO SOCIAL / CNPJ /ENDEREÇO COMPLETO / TELS. / E-mail
(Assinatura do representante legal da Proponente com a devida identificação)

ANEXO II - TERMO DE ACEITE DE PAGAMENTO

São Paulo, de de 202_.

CONTRATADA: [nome completo da empresa CONTRATADA]
CONTRATO ou PEDIDO: [número do contrato (e aditivo) ou Pedido]
OBJETO: [breve definição do objeto de contratação]

ATESTAMOS, para os devidos fins, que a **empresa [nome da empresa]**, procedeu com a **[prestação dos serviços ou entrega]** de **[apontar os serviços prestados ou produtos]**, discriminados na [Nota Fiscal Eletrônica de Serviço ou Nota Fiscal ou Nota Fiscal Fatura ou Fatura (no caso de locação)] n.º [inserir número], emitida em / / 202_, conforme doc. SEI nº [inserir o nº do doc. com hiperlink], referente ao [inserir o número do CO-00.00/0000 e TA-00.00/0000 ou PEDIDO], [dentro ou fora - Se fora do prazo, apontar a quantidade de dias] do prazo previsto, não havendo em nossos registros nenhum fato que desabone a conduta da empresa, respeitando as formalidades legais e cautelas de estilo, motivo pelo qual assinamos o presente termo, o que permite a adoção dos procedimentos de pagamento.

NOME DO GESTOR DA CONTRATAÇÃO
Cargo ou Função Gerência <detalhar> (XXX)

NOME DO FISCAL DA CONTRATAÇÃO
Cargo ou Função Gerência <detalhar> (XXX)

ANEXO III - TERMO DE ACEITE DOS SERVIÇOS DE IMPLANTAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO CLOUD WAF/WAAP

São Paulo, de de 202_.

CONTRATADA: [nome completo da empresa CONTRATADA]
CONTRATO ou PEDIDO: [número do contrato (e aditivo) ou Pedido]
OBJETO: [breve definição do objeto de contratação]

ATESTAMOS, para os devidos fins, que a empresa **[nome da empresa]**, procedeu com a Implantação e Configuração do(s) **[apontar os bens e produtos]**, discriminados na Nota Fiscal nº **[inserir número]**, emitida em / / 202_, conforme doc. SEI nº [inserir o nº do doc. com hiperlink], referente ao [inserir o número do CO-00.00/000 e TA-00.00/000 ou PEDIDO], em conformidade ao (à) [inserir o documento em que foram apresentadas as especificações técnicas (Requisição de Compra e/ou Termo de Referência)] e **[dentro ou fora]** do prazo previsto, não havendo em nossos registros nenhum fato que desabone a conduta da empresa, respeitando as formalidades legais e cautelas de estilo, motivo pelo qual assinamos o presente termo.

NOME DO GESTOR DA CONTRATAÇÃO
Cargo ou Função Gerência <detalhar> (XXX)

NOME DO FISCAL DA CONTRATAÇÃO
Cargo ou Função Gerência <detalhar> (XXX)

ANEXO IV - TERMO DE ACEITE DE RECEBIMENTO DAS LICENÇAS

São Paulo, de de 202_.

CONTRATADA: [nome completo da empresa CONTRATADA]

CONTRATO ou **PEDIDO:** [número do contrato (e aditivo) ou Pedido]

OBJETO: [breve definição do objeto de contratação]

ATESTAMOS, para os devidos fins, que a empresa [nome da empresa], procedeu com a Entrega da Licenças do(s) [apontar os bens e produtos], discriminados na Nota Fiscal nº [inserir número], emitida em / / 202_, conforme doc. SEI nº [inserir o nº do doc. com hiperlink], referente ao [inserir o número do CO-00.00/000 e TA-00.00/000 ou PEDIDO], em conformidade ao (à) [inserir o documento em que foram apresentadas as especificações técnicas (Requisição de Compra e/ou Termo de Referência)] e [dentro ou fora] do prazo previsto, não havendo em nossos registros nenhum fato que desabone a conduta da empresa, respeitando as formalidades legais e cautelas de estilo, motivo pelo qual assinamos o presente termo.

NOME DO GESTOR DA CONTRATAÇÃO

Cargo ou Função Gerência <detalhar> (XXX)

NOME DO FISCAL DA CONTRATAÇÃO

Cargo ou Função Gerência <detalhar> (XXX)

ANEXO V - TERMO DE ACEITE DE RECEBIMENTO DO TREINAMENTO

São Paulo, de de 202_.

CONTRATADA: [nome completo da empresa CONTRATADA]

CONTRATO ou **PEDIDO:** [número do contrato (e aditivo) ou Pedido]

OBJETO: [breve definição do objeto de contratação]

ATESTAMOS, para os devidos fins, que a empresa [nome da empresa], procedeu com o Treinamento do(s) [apontar os bens e produtos], discriminados na Nota Fiscal nº [inserir número], emitida em / / 202_, conforme doc. SEI nº [inserir o nº do doc. com hiperlink], referente ao [inserir o número do CO-00.00/000 e TA-00.00/000 ou PEDIDO], em conformidade ao (à) [inserir o documento em que foram apresentadas as especificações técnicas (Requisição de Compra e/ou Termo de Referência)] e [dentro ou fora] do prazo previsto, não havendo em nossos registros nenhum fato que desabone a conduta da empresa, respeitando as formalidades legais e cautelas de estilo, motivo pelo qual assinamos o presente termo.

NOME DO GESTOR DA CONTRATAÇÃO

Cargo ou Função Gerência <detalhar> (XXX)

NOME DO FISCAL DA CONTRATAÇÃO

Cargo ou Função Gerência <detalhar> (XXX)

**ANEXO VI - MODELO DE ORDEM DE SERVIÇO DE CONSULTORIA
(CONSULTORIA TÉCNICA ESPECIALIZADA - SOB DEMANDA)**

PREGÃO ELETRÔNICO NºXX.XXX/2026

CO-XX.XX/202_

1. IDENTIFICAÇÃO DA ORDEM DE SERVIÇO

Número da OS: _____

Data de emissão: ____ / ____ / ____

Contato responsável: _____

E-mail / Telefone: _____

Responsável técnico: _____

2. OBJETO DA ORDEM DE SERVIÇO

Prestação de serviços de Consultoria Técnica Especializada sob demanda.

3. ESCOPO DOS SERVIÇOS

(Descrever detalhadamente os serviços a serem executados)

() Tuning / Otimização

() Nova Implementação

() Mudança de Arquitetura

() Diagnóstico

() Outro: _____

5. ESTIMATIVA DE ESFORÇO

Horas estimadas: _____

Valor hora: R\$ _____

Valor total estimado da OS: R\$ _____

6. PRAZO DE EXECUÇÃO

Data início: ____ / ____ / ____

Data conclusão: ____ / ____ / ____

Horário: () Comercial () Fora do horário () Agendado

7. ENTREGÁVEIS

Plano de trabalho

Relatório técnico

Evidências de execução

8. Premissas e Restrições

Dependência de acesso ao ambiente

Aprovação prévia de mudanças críticas

Backup antes de alterações

10. ACEITE DA ESPECIFICAÇÃO

Pelo Prestador: _____

Assinatura: _____

Data: ____ / ____ / ____

12. FATURAMENTO E PAGAMENTO

O faturamento será realizado conforme seção Condições de Faturamento deste Termo de Referência.

O pagamento somente será efetuado após o ateste do gestor da O.S., caracterizando que a demanda foi atendida em perfeitas condições em relação às especificações e necessidades da PRODAM.

ANEXO VII - DECLARAÇÃO DE VISITA TÉCNICA

REF.: PREGÃO ELETRÔNICO NºXX.XXX/202_

ATESTO que o representante legal do licitante, inscrito no CNPJ sob o nº, interessado em participar do Pregão Eletrônico nº /_, Processo nº /_, realizou nesta data visita técnica nas instalações do, recebendo assim todas as informações e subsídios necessários para a elaboração da sua proposta.

O licitante está ciente desde já que, em conformidade com o estabelecido no Edital, não poderá pleitear em nenhuma hipótese modificações nos preços, prazos ou condições ajustadas, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou informações sobre os locais em que serão executados os serviços.

(local e data)

(nome completo, assinatura e qualificação do representante da licitante)

(nome completo, assinatura e cargo do servidor responsável por acompanhar a visita)	(nome completo, assinatura e cargo do servidor responsável pela contratação/licitação)
---	--

ANEXO VIII - TERMO DE ACEITE DA ORDEM DE SERVIÇO DE CONSULTORIA

São Paulo, de de 202_.

CONTRATADA: [nome completo da empresa CONTRATADA]

CONTRATO ou **PEDIDO:** [número do contrato (e aditivo) ou Pedido]

ORDEM DE SERVIÇO: [número da Ordem de Serviço de Consultoria]

OBJETO: [breve definição do objeto da Ordem de Serviço]

ATESTAMOS, para os devidos fins, que a empresa [nome da empresa], procedeu a prestação do(s) [serviços de consultoria], referentes a Ordem de Serviço nº [inserir número], emitida em / / 202_, conforme doc. SEI nº [inserir o nº do doc. com hiperlink], em conformidade ao (à) [inserir o documento em que foram apresentadas as especificações técnicas da Ordem de Serviço] e [dentro ou fora] do prazo previsto, não havendo em nossos registros nenhum fato que desabone a conduta da empresa, respeitando as formalidades legais e cautelas de estilo, motivo pelo qual assinamos o presente termo.

NOME DO GESTOR DA CONTRATAÇÃO

Cargo ou Função Gerência <detalhar> (XXX)

NOME DO FISCAL DA CONTRATAÇÃO

Cargo ou Função Gerência <detalhar> (XXX)



Wagner Kanagusuko

Gerente

Em 16/07/2026, às 15:15.

A autenticidade deste documento pode ser conferida no site <http://processos.prefeitura.sp.gov.br>, informando o código verificador **157670585** e o código CRC **E23E768B**.

V11.1

Referência: Processo nº 7010.2026/0005768-5

SEI nº 157670585