



**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

Setembro / 2026

1. OBJETO

Contratação de **solução Cloud WAF/WAAP**, prestada no **modelo SaaS**, para proteção de aplicações web e APIs, incluindo subscrição, implantação, configuração, integração, homologação, treinamento, suporte técnico e consultoria especializada, conforme os requisitos, capacidades e condições estabelecidos neste Termo de Referência e seus anexos. Não serão admitidas soluções que dependam de componentes de processamento instalados nos datacenters da CONTRATANTE.

2. TABELA DE COMPOSIÇÃO DOS ITENS

Item	Descrição	Unidade	Quantidade
1	Subscrição da solução Cloud WAF/WAAP por 36 meses, contados da emissão do Termo de Aceite dos Serviços de Implantação e Configuração, incluindo todas as licenças, módulos, capacidades, franquias, atualizações e demais recursos necessários ao atendimento integral do Ambiente Estimado de Referência.	Mês	36
2	Serviço de implantação, configuração completa, integração e homologação inicial da solução Cloud WAF/WAAP, incluindo ativação do tenant, parametrização, piloto, implantação da amostra definida para aceite, operação assistida e entrega da documentação técnica.	Serviço	1
3	Serviço continuado de suporte técnico e sustentação da solução Cloud WAF/WAAP por 36 meses, contados da emissão do Termo de Aceite dos Serviços de Implantação e Configuração.	Mês	36
4	Treinamento oficial da solução, compreendendo 6 (seis) vagas, utilizáveis em até 3 (três) turmas, agendas ou edições distintas.	Vaga	6
5	Consultoria Técnica Especializada sob demanda.	Hora técnica	300

2.1 Delimitação dos itens 1, 2 e 3

2.2 O item 1 compreende a subscrição da plataforma SaaS e os recursos fornecidos pelo fabricante como parte do licenciamento, incluindo licenças, módulos, capacidades, certificados, atualizações, regras gerenciadas, inteligência de ameaças, correções de segurança e suporte do fabricante quando inerente à subscrição.

2.3 O item 2 compreende todos os recursos e serviços necessários à implantação, integração, piloto, homologação e operação assistida, inclusive licenças, módulos, capacidades e suporte utilizados antes do aceite.

2.4 O item 3 compreende exclusivamente os serviços continuados prestados pela CONTRATADA, incluindo atendimento técnico, gestão de chamados,

diagnóstico, escalonamento, solução de contorno, acompanhamento e estabilização.

2.5 Não será admitida cobrança em duplicidade por recurso, atividade ou serviço incluído em mais de um item.

3. MODELO DE LICENCIAMENTO, DIMENSIONAMENTO E EQUIVALÊNCIA TÉCNICA

3.1 A solução deverá atender integralmente ao Ambiente Estimado de Referência, independentemente do modelo de licenciamento adotado pelo fabricante.

3.2 Serão admitidos modelos baseados em requisições processadas, aplicações ou FQDNs, APIs, throughput, módulos funcionais ou combinação dessas métricas.

3.3 A licitante deverá informar sua metodologia oficial de licenciamento e demonstrar que a proposta contempla todos os recursos necessários ao atendimento simultâneo das capacidades mínimas contratadas.

3.4 Definição de FQDN protegido

3.4.1 Considera-se FQDN protegido cada nome de domínio completo configurado e ativo na plataforma para recepção, inspeção e encaminhamento de tráfego HTTP ou HTTPS. Não serão contabilizados adicionalmente nomes técnicos internos, registros utilizados exclusivamente para validação de domínio ou emissão de certificados, health checks, identificadores internos ou FQDNs removidos ou desativados. Certificados wildcard ou multidomínio não alteram a quantidade de FQDNs protegidos.

3.4.2 A licitante deverá informar sua metodologia oficial de contabilização e eventuais situações de consumo adicional. A metodologia adotada não poderá reduzir a capacidade mínima de 700 FQDNs ativos e protegidos simultaneamente.

3.5 Definição de API protegida

3.5.1 Considera-se API protegida cada serviço lógico administrado como unidade independente de inventário ou política de segurança, identificado por especificação, contexto de publicação, base path ou versão. Endpoints e métodos HTTP da mesma API não serão contabilizados individualmente, salvo quando o modelo oficial do fabricante adotar métrica distinta. Nessa hipótese, a proposta deverá contemplar capacidade suficiente para proteger no mínimo 100 APIs, sem limitação incompatível de endpoints, métodos ou versões.

3.5.2 A licitante deverá informar a unidade comercial utilizada, os limites de endpoints e versões, o tratamento de diferentes ambientes e APIs descobertas automaticamente e as situações de contabilização adicional.

3.6 A equivalência técnica será aferida pela capacidade efetivamente comprovada, independentemente da métrica comercial ou do modelo de licenciamento do fabricante. A solução somente será considerada equivalente quando atender simultaneamente aos requisitos mínimos obrigatórios e às capacidades do Ambiente Estimado de Referência, não sendo admitida a

compensação da insuficiência de um requisito obrigatório por capacidade superior em outro. A comprovação será consolidada na Matriz de Conformidade, Capacidade e Equivalência Técnica (Anexo VIII).

3.7 Ambiente Estimado de Referência

3.7.1 Para fins de dimensionamento técnico, formação de preços e comparação das propostas, considera-se o seguinte Ambiente Estimado de Referência.

Métrica	Capacidade mínima incluída
FQDNs protegidos	700
APIs protegidas	100
Requisições processadas	7,78 bilhões/mês
RPS sustentado	3.000
RPS de pico	4.000
Throughput sustentado	1,5 Gbps
Throughput de pico	3 Gbps
Exportação de logs	1 TB/mês
Retenção de logs	30 dias

3.7.2 Os quantitativos, volumes e parâmetros do Ambiente Estimado de Referência possuem natureza estimativa e destinam-se ao dimensionamento, à formação dos preços e à comparação objetiva das propostas. Não constituem inventário definitivo, medição exata do ambiente atual ou garantia de consumo, devendo a proposta contemplar capacidade comercial compatível com esses valores, conforme o modelo oficial de licenciamento do fabricante.

3.7.3 Para fins de dimensionamento:

3.7.3.1 os valores de RPS e throughput representam capacidades técnicas para absorção de picos, não pressupõem utilização contínua e não serão somados à franquia mensal de requisições;

3.7.3.2 o volume de 7,78 bilhões de requisições por mês corresponde à capacidade mínima incluída no preço, sem garantia de consumo;

3.7.3.3 o consumo inferior não gerará saldo, compensação ou pagamento adicional;

3.7.3.4 o consumo superior somente poderá gerar cobrança mediante autorização prévia e formalização pela CONTRATANTE;

3.7.3.5 o atingimento de franquia ou capacidade comercial não poderá interromper, bloquear, limitar ou degradar automaticamente os serviços protegidos;

3.7.3.6 a CONTRATADA deverá disponibilizar alertas progressivos de consumo e comunicar a CONTRATANTE antes de qualquer medida que possa afetar a continuidade;

3.7.3.7 a solução deverá manter as capacidades contratadas durante todo o período dos itens recorrentes.

3.7.4 Quando o fabricante utilizar métrica distinta, a licitante deverá apresentar sua metodologia de equivalência e demonstrar que a proposta contempla capacidade compatível com todos os valores estimados.

3.8 Crescimento Estimado

3.8.1 Durante o período de prestação dos itens recorrentes, a solução deverá permitir expansão, sem substituição estrutural ou perda de configurações, até:

3.8.1.1 1.050 FQDNs;

3.8.1.2 150 APIs;

3.8.1.3 11,67 bilhões de requisições mensais;

3.8.1.4 6.000 RPS de pico;

3.8.1.5 2,25 Gbps de throughput sustentado;

3.8.1.6 10 TB mensais de exportação de logs.

3.8.2 As capacidades adicionais não estão incluídas no preço inicial, salvo declaração expressa da licitante. Sua contratação dependerá de solicitação formal, disponibilidade orçamentária, análise de vantajosidade e formalização contratual, podendo ocorrer por adição de licenças, subscrições ou recursos compatíveis, sem reinstalação integral ou indisponibilidade relevante.

3.8.3 Os preços de expansão informados na proposta permanecerão vinculantes durante o período dos itens recorrentes, sujeitos ao reajuste contratual. Quando a capacidade não for comercializada isoladamente, a licitante deverá informar o menor pacote, plano ou combinação de recursos capaz de atender à expansão, com o respectivo preço.

4. VIGÊNCIA

4.1 O contrato terá vigência de até 39 meses contados da assinatura, compreendendo o período de implantação e aceite, os 36 meses de prestação dos itens recorrentes e as obrigações de transição e encerramento contratual.

4.2 A implantação e a homologação deverão ser concluídas em até 50 dias corridos. Os itens recorrentes serão prestados por 36 meses contados da emissão do Termo de Aceite dos Serviços de Implantação e Configuração, sem ampliação do número de parcelas e sem faturamento anterior a esse marco.

4.3 O atraso imputável à CONTRATADA não gerará pagamento adicional ou prorrogação automática. Impedimentos comprovadamente causados pela CONTRATANTE poderão ensejar ajuste formal do cronograma e, quando necessário e juridicamente cabível, da vigência, sem alteração automática dos quantitativos ou valores.

4.4 A eventual prorrogação dos serviços recorrentes dependerá de justificativa, vantajosidade, disponibilidade orçamentária e observância da legislação e dos regulamentos aplicáveis.

5. CONTEXTO E JUSTIFICATIVA

5.1 A contratação tem por objetivo reforçar a proteção das aplicações web e APIs da Administração Municipal contra ataques abrangidos pelo OWASP Top 10 Web e OWASP API Security Top 10, ataques DDoS, bots maliciosos, automações abusivas e exploração de vulnerabilidades.

- 5.2 Busca-se padronizar a camada de segurança de aplicações, ampliar a disponibilidade e a observabilidade dos serviços digitais, apoiar a investigação de incidentes e atender às exigências legais, especialmente à Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD).
- 5.3 As capacidades foram estimadas com base no inventário disponível, nas projeções de crescimento, na sazonalidade e nos picos de utilização. A adoção do modelo SaaS visa proporcionar escalabilidade, atualização contínua, alta disponibilidade, mitigação distribuída de DDoS e menor dependência dos recursos computacionais da CONTRATANTE, sem indicação de fabricante ou produto específico.

6. ANÁLISE DE RISCOS, PRIVACIDADE E LGPD

- 6.1 Como condição para o aceite, a CONTRATADA deverá apresentar:
- 6.1.1 análise de riscos da solução;
 - 6.1.2 mapeamento dos fluxos de dados processados ou armazenados;
 - 6.1.3 localização dos ambientes e suboperadores envolvidos;
 - 6.1.4 prazos de retenção;
 - 6.1.5 medidas técnicas e administrativas de segurança.
- 6.2 Quando houver tratamento de dados pessoais, a CONTRATADA deverá fornecer as informações necessárias à elaboração ou atualização do Relatório de Impacto à Proteção de Dados Pessoais pela CONTRATANTE.

6.3 Comunicação e tratamento de incidentes

- 6.3.1 A CONTRATADA deverá comunicar, em até quatro horas da ciência, qualquer incidente confirmado ou sob investigação que possa afetar dados, logs, credenciais, configurações, tráfego ou serviços abrangidos pelo contrato.
- 6.3.2 A comunicação deverá conter, no mínimo:
- 6.3.2.1 data e hora da detecção;
 - 6.3.2.2 natureza do incidente;
 - 6.3.2.3 ambientes, serviços e dados potencialmente afetados;
 - 6.3.2.4 medidas de contenção;
 - 6.3.2.5 riscos identificados;
 - 6.3.2.6 responsável pelo acompanhamento;
 - 6.3.2.7 previsão da próxima atualização.
- 6.3.3 A CONTRATADA deverá fornecer atualizações até a contenção e apresentar relatório conclusivo, contendo causa-raiz e plano de prevenção, em até 10 dias úteis, salvo prazo aprovado pela CONTRATANTE. As evidências e a cadeia de custódia deverão ser preservadas. A utilização de fabricante, provedor ou suboperador não afasta a responsabilidade da CONTRATADA.

7. REQUISITOS TÉCNICOS DA SOLUÇÃO

7.1 Arquitetura

- 7.1.1 A solução deverá operar em arquitetura Cloud/SaaS, provida pelo fabricante ou parceiro autorizado, sem componentes de processamento instalados nos datacenters da CONTRATANTE.

7.1.2 A solução deverá disponibilizar ambiente lógico, organização, conta ou tenant próprio para a CONTRATANTE, com segregação de dados, configurações, políticas, credenciais, registros, logs e recursos administrativos em relação aos demais clientes do fabricante ou da CONTRATADA. Não deverá ser possível o acesso cruzado ou a exposição de informações entre ambientes de clientes distintos. Serão aceitas arquiteturas compartilhadas ou dedicadas, desde que atendidos os requisitos de segregação, segurança, desempenho, disponibilidade e privacidade estabelecidos neste Termo de Referência.

7.2 Compatibilidade com Ambiente Existente

7.2.1 A solução deverá interoperar com os balanceadores F5 BIG-IP i10600 utilizados pela CONTRATANTE, sem exigir sua substituição. A interoperabilidade poderá ocorrer pelo fluxo de tráfego entre a solução SaaS, os balanceadores e as aplicações de origem, sem exigência de integração proprietária, gerenciamento unificado ou compartilhamento de políticas, preservando, quando aplicável, as funções existentes de balanceamento, roteamento, alta disponibilidade, terminação SSL/TLS e encaminhamento de tráfego.

7.2.2 A CONTRATADA deverá apoiar a definição e a execução das alterações necessárias em DNS, certificados digitais, origens, cabeçalhos, regras de firewall e health checks, sem custo adicional.

7.3 Mitigação de ataques DDoS

7.3.1 A solução deverá proteger a infraestrutura de borda utilizada para recepção, inspeção e encaminhamento do tráfego dos FQDNs protegidos contra ataques DDoS nas camadas L3, L4 e L7, incluindo ataques volumétricos, floods HTTP/HTTPS e ataques de exaustão de recursos.

7.3.2 Não integra o objeto a proteção direta dos links de comunicação, dos blocos de endereçamento IP ou de protocolos não encaminhados pela solução SaaS, salvo quando essa capacidade estiver expressamente incluída na proposta.

7.3.3 A mitigação deverá:

7.3.3.1 ocorrer na infraestrutura distribuída da solução;

7.3.3.2 impedir que ataques dirigidos aos endereços publicados pela plataforma afetem os serviços protegidos;

7.3.3.3 permanecer ativa durante todo o evento, sem limitação artificial de duração;

7.3.3.4 não gerar cobrança decorrente exclusivamente do volume de tráfego malicioso mitigado, observadas as condições comerciais apresentadas na proposta.

7.3.4 Durante a implantação, a CONTRATADA deverá apresentar documentação de arquitetura contendo:

7.3.4.1 o fluxo de tráfego em condições normais e durante eventos DDoS;

7.3.4.2 os mecanismos de proteção dos endereços da plataforma;

7.3.4.3 os mecanismos de restrição de acesso direto às origens;

7.3.4.4 as responsabilidades da CONTRATANTE para prevenção de bypass da solução.

7.4 Inteligência contra bots e automações

- 7.4.1 A solução deverá identificar, classificar e mitigar bots e automações abusivas, diferenciando, quando tecnicamente possível, usuários legítimos, bots autorizados e automações maliciosas.
- 7.4.2 A identificação deverá utilizar análise comportamental, fingerprinting, inteligência de ameaças ou mecanismos equivalentes, permitindo a detecção de automações distribuídas e de técnicas de evasão, como headless browsers, spoofing e rotação de endereços IP.
- 7.4.3 A solução deverá oferecer mecanismos para detecção ou mitigação de, no mínimo:
 - 7.4.3.1 credential stuffing e brute force distribuído;
 - 7.4.3.2 scraping automatizado;
 - 7.4.3.3 criação automatizada de contas;
 - 7.4.3.4 account takeover;
 - 7.4.3.5 abuso automatizado de aplicações e APIs.
- 7.4.4 A solução deverá permitir a aplicação de ações diferenciadas conforme a classificação do tráfego, incluindo:
 - 7.4.4.1 monitoramento;
 - 7.4.4.2 limitação de requisições;
 - 7.4.4.3 aplicação de desafios;
 - 7.4.4.4 bloqueio.
- 7.4.5 A solução deverá permitir a criação de políticas diferenciadas por aplicação, API, endpoint, origem, sessão ou atributo equivalente suportado pelo fabricante.
- 7.4.6 O processamento de tráfego, metadados e eventos de segurança deverá observar as seções Análise de Riscos, Privacidade e LGPD e Tratamento, Retenção e Soberania dos Dados.

7.5 Desempenho, Capacidade e Escalabilidade

- 7.5.1 A solução deverá atender às capacidades estabelecidas no Ambiente Estimado de Referência, com as funções obrigatórias de inspeção, proteção e terminação SSL/TLS ativas, e deverá:
 - 7.5.1.1 suportar TLS 1.2 e TLS 1.3;
 - 7.5.1.2 realizar o processamento criptográfico do tráfego HTTPS;
 - 7.5.1.3 processar aplicações web, APIs REST e conteúdo JSON;
 - 7.5.1.4 absorver as variações e os picos de tráfego definidos neste Termo de Referência;
 - 7.5.1.5 manter as funções essenciais de proteção durante eventos de ataque;
 - 7.5.1.6 permitir a expansão prevista na subseção Crescimento Estimado sem substituição estrutural ou perda de configurações.
- 7.5.2 As capacidades, métricas comerciais e regras de equivalência observarão a seção Modelo de Licenciamento, Dimensionamento e Equivalência Técnica.

7.6 Avaliação de impacto no desempenho

- 7.6.1 Durante a homologação será avaliado o impacto funcional da solução sobre pelo menos uma aplicação da amostra. Quando tecnicamente possível, serão comparados o fluxo sem passagem pela solução e o fluxo protegido, utilizando a mesma aplicação, operação e origem de teste.
- 7.6.2 Serão registrados a quantidade de requisições, os tempos de resposta, os erros HTTP, os timeouts e as falhas de conexão. A avaliação terá por finalidade identificar indisponibilidade, erro recorrente ou degradação que impeça o uso normal da aplicação e seja comprovadamente causada pela solução ou por sua configuração.
- 7.6.3 Em caso de divergência entre as equipes ou ocorrência atribuível à solução, será realizada nova execução controlada após os ajustes necessários. As métricas observadas serão registradas como linha de base operacional.
- 7.6.4 Não será exigido limite fixo de latência durante a homologação.

7.7 Métricas de Consumo e Capacidade

- 7.7.1 Para dimensionamento e acompanhamento do consumo, será considerada a quantidade de requisições HTTP ou HTTPS processadas. Quando o fabricante utilizar outra métrica comercial, a licitante deverá informar a metodologia oficial de medição e equivalência e demonstrar que a proposta contempla as capacidades contratadas.
- 7.7.2 Considera-se processada cada requisição submetida aos mecanismos de inspeção e proteção, independentemente de ter sido permitida, bloqueada, mitigada, desafiada ou redirecionada. A mesma requisição não poderá ser contabilizada mais de uma vez pela atuação simultânea ou sequencial de diferentes módulos.
- 7.7.3 Não serão contabilizados adicionalmente:
 - 7.7.3.1 retries, retransmissões ou comunicações internas da plataforma;
 - 7.7.3.2 health checks ou monitoramentos gerados pela solução;
 - 7.7.3.3 sub-requisições técnicas;
 - 7.7.3.4 chamadas de desafio geradas pela plataforma;
 - 7.7.3.5 transferências entre a plataforma e a origem;
 - 7.7.3.6 registros do mesmo evento por diferentes módulos.
- 7.7.4 A licitante deverá declarar a metodologia aplicável a redirecionamentos, WebSocket, GraphQL, requisições bloqueadas antes do encaminhamento à origem, validação de certificados e monitoramentos realizados pela CONTRATANTE. Essa metodologia deverá ser considerada no dimensionamento e no preço.

7.8 Preservação do IP de Origem

- 7.8.1 A solução deverá disponibilizar ao backend o endereço IP original do cliente final por X-Forwarded-For, True-Client-IP ou mecanismo equivalente oficialmente suportado, com validação contra spoofing.
- 7.8.2 A documentação de arquitetura entregue no aceite deverá descrever o fluxo e os mecanismos utilizados.

7.9 Bloqueio por IP de Origem em Cenários sem Preservação do IP

- 7.9.1 Quando uma aplicação legada não puder utilizar diretamente o

mecanismo de preservação do IP original, a solução deverá permitir a aplicação de políticas de bloqueio e controle de acesso na própria camada WAF/WAAP, com base no endereço observado, em cabeçalhos confiáveis, metadados, informações de sessão ou mecanismo equivalente.

- 7.9.2 A aplicação das políticas não deverá depender de alteração de código, salvo quando tecnicamente indispensável e previamente aprovada pela CONTRATANTE. A viabilidade será comprovada conforme a Matriz de Conformidade e, quando aplicável, durante a homologação.

7.10 Funcionalidades de Proteção de Aplicações Web e APIs (WAAP)

- 7.10.1 A solução deverá oferecer, no mínimo:

- 7.10.1.1 proteção contra riscos tecnicamente tratáveis do OWASP Top 10 Web;
- 7.10.1.2 descoberta e inventário de APIs expostas, inclusive APIs não documentadas ou desatualizadas, quando tecnicamente identificáveis;
- 7.10.1.3 importação ou utilização de especificações OpenAPI/Swagger;
- 7.10.1.4 validação de schema;
- 7.10.1.5 criação de políticas por API, endpoint ou método HTTP;
- 7.10.1.6 rate limiting e controle de burst por origem, aplicação, API ou endpoint;
- 7.10.1.7 virtual patching para vulnerabilidades conhecidas;
- 7.10.1.8 mecanismos de detecção, mitigação, alerta ou aplicação de políticas para os riscos tecnicamente tratáveis do OWASP API Security Top 10;
- 7.10.1.9 inteligência de ameaças atualizada pelo fabricante;
- 7.10.1.10 criação de regras e políticas customizadas.

- 7.10.2 Para riscos dependentes da lógica de negócio, da identidade, da autorização ou da implementação interna da aplicação, serão aceitos mecanismos de descoberta, análise comportamental, correlação de eventos, alertas, rate limiting e políticas customizadas.

- 7.10.3 A solução deverá oferecer mecanismos compatíveis com a camada WAAP para identificação ou mitigação de anomalias relacionadas a sessões, cookies e reutilização indevida de tokens, quando as informações necessárias estiverem disponíveis à plataforma.

7.11 Gerenciamento Automatizado de Certificados Digitais SSL/TLS

- 7.11.1 A solução deverá fornecer e gerenciar certificados SSL/TLS públicos e confiáveis para os FQDNs protegidos, sem aquisição separada ou custo adicional.

- 7.11.2 O gerenciamento deverá contemplar:

- 7.11.2.1 emissão e instalação;
- 7.11.2.2 validação de domínio;
- 7.11.2.3 renovação automática;
- 7.11.2.4 substituição e, quando aplicável à autoridade certificadora utilizada, revogação;
- 7.11.2.5 monitoramento de validade;
- 7.11.2.6 alertas de falha;
- 7.11.2.7 trilhas de auditoria.

- 7.11.3 As operações ordinárias do ciclo de vida deverão ocorrer automaticamente, sem geração manual periódica de CSR ou abertura de chamados.

- 7.11.4 A solução deverá suportar certificados individuais por FQDN,

certificados multidomínio ou wildcard e certificados fornecidos pela CONTRATANTE, conforme sua necessidade.

7.11.5 As chaves privadas deverão ser protegidas por controles criptográficos, segregação de acesso e auditoria.

7.11.6 A solução deverá disponibilizar inventário dos certificados, incluindo FQDN, emissor, validade, estado de renovação e eventuais falhas.

7.11.7 A CONTRATADA deverá assegurar a continuidade do ciclo de vida dos certificados durante todo o período de prestação dos itens recorrentes, inclusive diante de alterações dos padrões aplicáveis.

7.12 Operação, Observabilidade e Integração

7.12.1 A solução deverá permitir integração com SIEM/SOAR por syslog, CEF, LEEF, API ou mecanismo equivalente oficialmente suportado, em tempo próximo ao real e sem desenvolvimento customizado oneroso.

7.12.2 Os eventos deverão conter, quando aplicável, timestamp, IP de origem, método HTTP, URI ou endpoint, código de resposta, ação aplicada, regra acionada e severidade.

7.12.3 A solução deverá disponibilizar métricas de tráfego, latência, códigos HTTP e eventos de segurança, APIs para administração e automação e relatórios técnicos e executivos.

7.13 Logs, Auditoria e Retenção

7.13.1 A solução deverá permitir:

7.13.1.1 retenção mínima de 30 dias para logs de segurança e eventos operacionais;

7.13.1.2 exportação de até 1 TB por mês para sistemas externos;

7.13.1.3 diferenciação entre logs operacionais, de segurança e de APIs;

7.13.1.4 mecanismo que permita o reenvio, a recuperação ou a nova consulta aos eventos em caso de indisponibilidade temporária do destino, enquanto os eventos estiverem abrangidos pelo período de retenção.

7.13.2 A franquia de exportação de 1 TB por mês refere-se aos logs e eventos selecionados pela CONTRATANTE e não implica exportação individual de todas as requisições processadas. A solução deverá permitir filtragem por aplicação, categoria, severidade e ação, emitir alertas de consumo e não interromper a proteção do tráfego em razão do atingimento da franquia.

7.13.3 A retenção poderá utilizar armazenamento nativo, solução externa incluída na proposta ou, mediante aprovação da CONTRATANTE, ambiente sob seu controle, desde que asseguradas integridade, confidencialidade e disponibilidade. A licitante deverá indicar a localização da retenção, os recursos incluídos e as dependências da CONTRATANTE.

7.13.4 Eventual utilização de amostragem deverá ser informada na proposta, com indicação das categorias de registros afetadas.

7.13.5 A retenção por prazo superior a 30 dias poderá ser realizada pela CONTRATANTE em seu SIEM ou armazenamento, mediante os mecanismos de exportação previstos neste Termo de Referência.

7.13.6 A proposta deverá incluir todos os custos de geração, processamento, armazenamento temporário, transferência, egress e conectores necessários à exportação de até 1 TB por mês, sem contabilização duplicada ou faturamento de excedente não previamente autorizado.

- 7.13.7 A CONTRATADA deverá disponibilizar relatório mensal contendo o volume de logs exportados, o consumo da franquia e as falhas relevantes de entrega identificadas.

7.14 Alta Disponibilidade (HA) e Continuidade Operacional

- 7.14.1 A solução deverá operar em arquitetura de alta disponibilidade, com redundância e recuperação automática compatíveis com o modelo SaaS ofertado.
- 7.14.2 Serão admitidas arquiteturas baseadas em CDN, Anycast, balanceamento global, múltiplos PoPs, redundância regional, topologia ativo/ativo, ativo/passivo ou mecanismo equivalente.
- 7.14.3 A arquitetura deverá assegurar:
- 7.14.3.1 continuidade do encaminhamento e da proteção do tráfego diante de falhas de componentes;
 - 7.14.3.2 preservação das políticas e configurações;
 - 7.14.3.3 recuperação automática ou convergência sem intervenção manual ordinária;
 - 7.14.3.4 ausência de bypass não autorizado das funções de proteção.
- 7.14.4 A licitante deverá descrever os mecanismos de detecção de falha, retirada de rota, convergência e restabelecimento aplicáveis à solução.
- 7.14.5 A solução deverá possuir mecanismos documentados de redundância, recuperação, preservação das configurações, contingência e rollback. A comprovação da infraestrutura SaaS ocorrerá conforme a Matriz de Conformidade, sem provocação de indisponibilidade em PoPs, regiões, rotas ou componentes compartilhados do fabricante.

7.15 Administração Segura

- 7.15.1 A solução deverá oferecer, no mínimo:
- 7.15.1.1 MFA e RBAC;
 - 7.15.1.2 SSO (SAML ou OIDC);
 - 7.15.1.3 trilhas de auditoria e controle de alterações;
 - 7.15.1.4 registros auditáveis de acessos, alterações e eventos.
- 7.15.2 A solução deverá permitir a segregação lógica e administrativa dos ativos protegidos por aplicação, grupo de aplicações, ambiente, unidade organizacional ou escopo equivalente, possibilitando a atribuição de permissões diferenciadas aos usuários por meio de RBAC ou mecanismo equivalente. Um usuário não deverá visualizar, alterar ou administrar ativos fora dos escopos para os quais tenha sido autorizado.
- 7.15.3 A solução deverá permitir a criação e administração de múltiplos espaços lógicos segregados, tais como subtenants, organizações, contas, grupos administrativos, workspaces ou mecanismo equivalente, vinculados ao tenant principal da CONTRATANTE. Cada espaço deverá permitir, conforme as capacidades da plataforma, segregação de ativos protegidos, políticas, usuários, funções administrativas, registros de auditoria e relatórios, sem impedir a administração centralizada pela CONTRATANTE.
- 7.15.4 Não será exigida nomenclatura específica de “subtenant”. Será considerado equivalente qualquer mecanismo que assegure os resultados de segregação, delegação administrativa, visibilidade centralizada e

controle de acesso definidos neste Termo de Referência.

7.15.5 A licitante deverá informar a quantidade de espaços lógicos incluída na proposta, os limites aplicáveis e eventual impacto no licenciamento.

7.15.6 A integração efetiva com o provedor de identidade da CONTRATANTE será realizada durante a implantação quando os acessos, metadados e configurações necessários estiverem disponíveis. A indisponibilidade desses elementos por responsabilidade da CONTRATANTE não impedirá o aceite, desde que esteja comprovado o suporte da solução ao protocolo exigido.

8. CONSULTORIA TÉCNICA ESPECIALIZADA

8.1 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:

- 8.1.1 ajustes finos (tuning) da solução;
- 8.1.2 implementação de novas aplicações ou APIs;
- 8.1.3 criação e revisão de políticas de segurança;
- 8.1.4 mudanças de arquitetura ou topologia;
- 8.1.5 apoio técnico em incidentes complexos;
- 8.1.6 evolução contínua da solução.

8.2 O quantitativo de 300 horas possui natureza estimada e será utilizado exclusivamente mediante Ordem de Serviço previamente emitida e aprovada. O faturamento corresponderá às horas efetivamente executadas, comprovadas e aceitas, limitado ao quantitativo autorizado e ao saldo contratual. Horas não utilizadas não gerarão pagamento, compensação ou indenização.

8.3 A proposta deverá apresentar valor unitário por hora técnica, aplicável independentemente da atividade executada.

8.4 Não será admitido acréscimo de valor pela execução em período noturno, finais de semana ou feriados quando a necessidade decorrer de atividade prevista e autorizada na respectiva Ordem de Serviço.

8.5 A CONTRATADA deverá iniciar o atendimento da Ordem de Serviço no prazo definido nela, conforme criticidade, complexidade e disponibilidade dos acessos necessários.

8.6 Não poderão consumir horas de consultoria as atividades de suporte, correção de falhas ou não conformidades, cumprimento de requisito obrigatório ou ajustes decorrentes da implantação.

9. SEGURANÇA DO FABRICANTE E DA CADEIA DE SUPRIMENTOS

9.1 A CONTRATADA deverá comprovar que o fabricante mantém:

- 9.1.1 política pública de gerenciamento e divulgação responsável de vulnerabilidades;
- 9.1.2 processo de classificação, comunicação, correção e mitigação baseado em risco;
- 9.1.3 base pública de CVEs ou avisos de segurança;

- 9.1.4 atualizações de segurança durante o período dos itens recorrentes;
 - 9.1.5 controles de segurança do código-fonte e da cadeia de desenvolvimento;
 - 9.1.6 processo de gestão de vulnerabilidades em componentes de terceiros e de código aberto;
 - 9.1.7 certificação ISO/IEC 27001, ISO/IEC 27701, SOC 2 Type II ou equivalente.
- 9.2 Na ausência de correção imediata, deverão ser adotados controles compensatórios, comunicação formal, acompanhamento e plano de ação. Vulnerabilidades críticas com impacto confirmado ou exploração ativa deverão ser comunicadas à CONTRATANTE em até 24 horas da confirmação de impacto sobre a solução contratada.

10. SUPORTE TÉCNICO E SUSTENTAÇÃO

- 10.1 Os serviços recorrentes de suporte técnico e sustentação abrangerão todos os componentes da solução e serão prestados em regime 24x7 durante os 36 meses contados da emissão do Termo de Aceite dos Serviços de Implantação e Configuração.
- 10.2 A abertura de chamados poderá ser realizada por meio de portal, telefone, e-mail ou outro meio oficialmente disponibilizado pela CONTRATADA.
- 10.3 A CONTRATADA deverá disponibilizar atendimento técnico em língua portuguesa para abertura, acompanhamento e tratamento dos chamados.
- 10.4 A CONTRATADA deverá garantir atendimento contínuo aos chamados S1 e S2 até a implementação da solução de contorno ou estabilização do serviço, inclusive em períodos noturnos, finais de semana e feriados, salvo autorização formal da CONTRATANTE para suspensão ou alteração do regime de atendimento.

11. ACORDO DE NÍVEL DE SERVIÇO (SLA)

- 11.1 Os níveis de serviço relativos à subscrição, disponibilidade, suporte técnico e sustentação serão apurados a partir da emissão do Termo de Aceite dos Serviços de Implantação e Configuração.
- 11.2 Durante a implantação, o cumprimento das obrigações será avaliado pelos marcos do cronograma, pelo Plano de Trabalho e pelas penalidades específicas do item 2.

11.3 Classificação de Severidade

- 11.3.1 Os chamados de suporte serão inicialmente classificados pela equipe técnica da CONTRATANTE conforme os níveis a seguir. A classificação poderá ser ajustada mediante justificativa técnica registrada no chamado.

11.3.2 Severidade Alta (S1) - Incidente Crítico

- 11.3.2.1 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.

11.3.3 Severidade Média (S2) - Incidente Relevante

11.3.3.1 Aplica-se à indisponibilidade parcial da solução, falhas em funcionalidades relevantes ou degradação significativa de desempenho.

11.3.4 Severidade Baixa (S3) - Incidente Não Crítico

11.3.4.1 Aplica-se a falhas pontuais, dúvidas operacionais, ajustes de configuração ou problemas sem impacto relevante.

11.3.4.2 Os chamados S3 poderão ser registrados a qualquer momento. Os respectivos prazos serão apurados em horas úteis, não sendo contabilizados sábados, domingos e feriados, salvo atendimento expressamente autorizado pela CONTRATANTE.

11.4 Tempos Máximos de Atendimento

Severidade	Início do Atendimento	Prazo Máximo para Solução de Contorno	Prazo para Solução Definitiva ou Plano de Ação
Alta (S1)	até 1 (uma) hora	até 4 (quatro) horas corridas	Plano de ação: até 8 (oito) horas corridas. Solução definitiva: conforme criticidade e cronograma aprovado formalmente pela CONTRATANTE. O plano de ação deverá conter prazo de conclusão, responsável pela execução e forma de acompanhamento pela CONTRATANTE
Média (S2)	até 1 (uma) hora	até 8 (oito) horas corridas	Plano de ação: até 16 (dezesesseis) horas corridas. Solução definitiva: conforme criticidade e cronograma aprovado formalmente pela CONTRATANTE. O plano de ação deverá conter prazo de conclusão, responsável pela execução e forma de acompanhamento pela CONTRATANTE
Baixa (S3)	até 4 (quatro) horas úteis	até 9 (nove) horas úteis	solução definitiva ou plano de ação: até 24 (vinte e quatro) horas úteis

11.4.1 Para S1 e S2, o prazo da solução definitiva será aquele registrado no plano de ação aprovado pela CONTRATANTE. Para S3, será admitido plano de ação tecnicamente justificado quando a solução depender de correção, atualização ou ciclo de desenvolvimento do fabricante.

11.4.2 A CONTRATANTE analisará o plano de ação em até 4 horas corridas

para S1, 8 horas corridas para S2 e 2 dias úteis para S3, podendo aprová-lo, solicitar complementações ou estabelecer prazo compatível com a criticidade. A solicitação de complementação não suspenderá a manutenção da solução de contorno nem a investigação.

- 11.4.3 A CONTRATADA deverá acompanhar o chamado e informar sua evolução até a solução definitiva. A glosa por atraso do plano de ação será contada após 8 horas para S1 ou 16 horas para S2, e a glosa pela solução definitiva somente após o vencimento do prazo aprovado.

11.5 Disponibilidade da Solução

- 11.5.1 A solução WAF/WAAP deverá garantir disponibilidade mínima mensal de 99,95% para a infraestrutura responsável pela recepção, inspeção e encaminhamento do tráfego protegido. Falhas em funcionalidades administrativas que não afetem o tráfego protegido serão tratadas conforme os prazos de suporte.

- 11.5.2 A disponibilidade mensal será calculada pela seguinte fórmula:

$$11.5.3 \text{ Disponibilidade mensal (\%)} = [(TMM - TIM) \div TMM] \times 100$$

- 11.5.4 Onde:

- 11.5.5 **TMM** corresponde ao total de minutos do mês;

- 11.5.6 **TIM** corresponde ao total de minutos de indisponibilidade imputável à CONTRATADA.

- 11.5.7 O cálculo será realizado sem arredondamentos intermediários, e o percentual final de disponibilidade será considerado com três casas decimais, mediante arredondamento matemático.

- 11.5.8 Será considerado início da indisponibilidade o primeiro registro válido produzido pelas ferramentas de monitoramento da CONTRATANTE, da CONTRATADA ou do fabricante, prevalecendo o horário mais antigo tecnicamente comprovado.

- 11.5.9 Será considerado encerramento da indisponibilidade o momento em que o tráfego e os mecanismos de proteção forem comprovadamente restabelecidos.

- 11.5.10 Será considerada indisponibilidade, ainda que o tráfego continue sendo encaminhado, a falha que implique bypass não autorizado, ausência integral de inspeção ou perda das funções essenciais de proteção contratadas.

- 11.5.11 A indisponibilidade parcial será contabilizada pela multiplicação da duração do evento pelo percentual dos serviços críticos afetados, conforme o inventário e os pesos definidos no Plano de Trabalho. A soma dos pesos corresponderá a 100%, e falhas em componentes compartilhados serão atribuídas aos serviços por elas impactados.

- 11.5.12 Até a aprovação do inventário e dos pesos, o percentual afetado será calculado pela proporção entre a quantidade de serviços críticos afetados e o total de serviços críticos ativos. Alterações posteriores dos pesos dependerão de justificativa técnica e aprovação formal, sem efeitos retroativos.

- 11.5.13 Não serão excluídos do cálculo eventos decorrentes de falha de subcontratantes, provedores de nuvem, CDN, operadoras ou componentes utilizados pela CONTRATADA para prestação do objeto.

- 11.5.14 Poderão ser excluídos:
- 11.5.15 períodos de manutenção programada previamente autorizados;
- 11.5.16 falhas comprovadamente causadas pela CONTRATANTE;
- 11.5.17 indisponibilidade exclusiva da aplicação de origem, sem falha da solução WAF/WAAP;
- 11.5.18 casos de força maior, devidamente demonstrados e reconhecidos pela CONTRATANTE.
- 11.5.19 As manutenções programadas não poderão exceder quatro horas por mês e deverão ser comunicadas com antecedência mínima de cinco dias úteis. Somente será excluído do cálculo o intervalo previamente autorizado e efetivamente utilizado, não abrangendo períodos excedentes, falhas anteriores ou posteriores à janela, manutenções emergenciais imputáveis à CONTRATADA ou interrupções evitáveis pelos mecanismos ordinários de redundância.
- 11.5.20 A CONTRATADA deverá disponibilizar relatórios mensais de disponibilidade, contendo o registro detalhado dos eventos de indisponibilidade, suas causas e tempos de resolução.

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

12.1 Para fins desta seção, considera-se **Valor Mensal Afetado (VMA)** a parcela mensal do item 1, do item 3 ou de ambos, conforme o componente contratual diretamente relacionado ao descumprimento tecnicamente caracterizado.

12.2 Glosas por Indisponibilidade Mensal

Disponibilidade apurada	Glosa sobre o Valor Mensal Afetado (VMA)
Igual ou superior a 99,95%	Sem glosa
De 99,90% a 99,949%	2%
De 99,50% a 99,899%	5%
De 99,00% a 99,499%	10%
Inferior a 99,00%	15%

12.3 Glosas de Pagamento (Descumprimento de SLA)

12.3.1 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.

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

12.4 Atraso no Início do Atendimento

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

12.4.1.1 **0,1% por hora de atraso**, calculada sobre o Valor Mensal

Afetado (VMA) para qualquer nível de severidade.

12.5 Atraso na Solução de Contorno, Definitiva ou no Plano de Ação

12.5.1 Serão aplicadas glosas progressivas conforme a severidade:

12.5.2 **Severidade Alta (S1):** 2% por hora de atraso, calculada sobre o Valor Mensal Afetado (VMA);

12.5.3 **Severidade Média (S2):** 1% por hora de atraso, calculada sobre o Valor Mensal Afetado (VMA);

12.5.4 **Severidade Baixa (S3):** 0,5% por hora útil de atraso, calculada sobre o Valor Mensal Afetado (VMA).

12.5.5 Para cálculo das glosas, as frações de hora serão apuradas proporcionalmente por minuto, observada a natureza de hora corrida ou hora útil aplicável à severidade do chamado.

12.5.6 Para chamados S3, a apresentação tempestiva de plano de ação tecnicamente justificado atenderá ao prazo previsto na tabela de níveis de serviço. A glosa relativa à solução definitiva somente será aplicável após o vencimento do prazo estabelecido no plano de ação aceito pela CONTRATANTE.

12.6 Limite de Glosas e Reincidência

12.6.1 O somatório das glosas em um mesmo período de faturamento ficará limitado a 30% do VMA, e nenhum evento individual poderá gerar glosa superior a 15% do VMA.

12.6.2 A ocorrência de dois ou mais descumprimentos S1 em 90 dias ou de três ou mais descumprimentos da mesma severidade em 12 meses poderá ensejar procedimento administrativo para avaliação de falha contratual grave, observados o contraditório e a ampla defesa.

12.6.3 A aplicação dos limites de glosa não impede a apuração das sanções administrativas cabíveis por descumprimento grave ou reiterado.

12.7 Multas Contratuais (Sanção Administrativa)

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

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

12.7.2.1 atraso na implantação e configuração da solução;

12.7.2.2 atraso no início dos treinamentos;

12.7.2.3 atraso na emissão de certificados de conclusão;

12.7.2.4 descumprimento de obrigações contratuais relevantes.

12.8 Multas por Atrasos Contratuais

12.8.1 Aplicam-se as seguintes multas:

12.8.1.1 **1% (um por cento) por dia de atraso** na implantação e configuração da solução, calculado sobre o valor do serviço correspondente;

12.8.1.2 **1% (um por cento) por mês de atraso** no início dos

treinamentos, calculado sobre o valor total do item de treinamento;

12.8.1.3 0,5% (zero vírgula cinco por cento) sobre o valor do item de treinamento, em caso de atraso na emissão de certificados.

12.9 Não Cumulatividade

12.9.1 Para um mesmo evento gerador:

12.9.1.1 não haverá aplicação cumulativa entre glosa e multa;

12.9.1.2 será aplicada a medida mais gravosa, conforme análise da CONTRATANTE.

12.9.2 Múltiplos chamados decorrentes da mesma causa-raiz e do mesmo período de indisponibilidade serão considerados um único evento para fins de limite individual de glosa, sem prejuízo da contabilização do impacto sobre os diferentes serviços afetados.

12.9.3 Quando um mesmo evento caracterizar simultaneamente descumprimento de disponibilidade e atraso de atendimento, será aplicada a glosa de maior valor, vedada a dupla incidência sobre o mesmo fato gerador.

12.10 Disposições Gerais

12.10.1 As glosas incidirão diretamente no faturamento mensal, enquanto as multas dependerão de procedimento administrativo específico. As regras desta seção deverão ser interpretadas de forma sistemática, prevalecendo a disposição mais específica e observando-se a legislação aplicável. O limite das glosas não afasta outras penalidades administrativas cabíveis.

13. SERVIÇO DE IMPLANTAÇÃO E CONFIGURAÇÃO

13.1 Serviço de Implantação e Configuração de Toda a Solução

13.1.1 A implantação inicial da amostra, a operação assistida, a homologação e a entrega das respectivas evidências deverão ser concluídas em até 50 dias corridos contados da assinatura, observados os seguintes marcos:

13.1.1.1 reunião inicial e elaboração do Plano de Trabalho: até 5 dias úteis;

13.1.1.2 disponibilização do tenant, contas, licenças e subscrições: até 10 dias corridos;

13.1.1.3 configuração, integração, piloto e entrada em produção da amostra: até 30 dias corridos;

13.1.1.4 operação assistida: mínimo de 10 dias úteis após a entrada em produção;

13.1.1.5 conclusão das atividades e entrega das evidências de homologação: até 50 dias corridos.

13.1.2 Os marcos intermediários poderão ser ajustados no Plano de Trabalho, desde que não seja ultrapassado o prazo máximo total e que a alteração seja aprovada pela CONTRATANTE.

13.1.3 O início dos itens recorrentes e seu faturamento observarão as seções Vigência, Aceite e Condições de Faturamento.

13.1.4 A operação assistida integra o item 2 e terá duração mínima de 10 dias úteis após a entrada em produção da amostra. Nesse período, a CONTRATADA deverá acompanhar eventos, ajustar políticas e corrigir

falsos positivos, falsos negativos e demais não conformidades identificadas. A ausência de ocorrência durante o período não impedirá sua conclusão, desde que a solução permaneça operacional e os resultados sejam registrados.

13.1.5 Ao término, a CONTRATADA deverá apresentar relatório contendo os ativos acompanhados, eventos relevantes, ajustes realizados, pendências e situação final da amostra.

13.1.6 Os prazos das atividades afetadas serão suspensos pelo período estritamente necessário quando houver impedimento comprovadamente causado pela CONTRATANTE. A suspensão dependerá de comunicação formal da CONTRATADA contendo as evidências, atividades afetadas, impacto no cronograma e medidas de contingência, e não será aplicável quando o impedimento puder ser contornado sem risco, prejuízo ou custo adicional à CONTRATANTE.

13.1.7 A suspensão ou o ajuste do cronograma não implicará prorrogação automática da vigência, que dependerá de formalização específica quando necessária e juridicamente cabível.

13.2 Amostra mínima para implantação e homologação

13.2.1 A implantação inicial contemplará uma amostra de até **5 (cinco) FQDNs e 2 (duas) APIs**, selecionada pela CONTRATANTE durante a elaboração do Plano de Trabalho, observados os limites e perfis estabelecidos abaixo.

13.2.2 Os quantitativos do Ambiente Estimado de Referência representam capacidade contratada e não implicam a obrigação de incorporar todos os FQDNs e APIs durante a implantação inicial.

13.2.3 Sempre que disponíveis, a amostra deverá incluir ativos que permitam avaliar aplicação crítica, aplicação legada, autenticação, API REST, especificação OpenAPI/Swagger e integração com os balanceadores existentes. Um mesmo FQDN ou API poderá atender a mais de um desses perfis, desde que permita a execução dos testes aplicáveis.

13.2.4 A indisponibilidade de ativo com algum dos perfis indicados não impedirá a homologação, desde que essa condição seja registrada no Plano de Trabalho e não impossibilite a execução dos testes funcionais essenciais.

13.2.5 A seleção dos ativos será realizada pela CONTRATANTE e formalizada no Plano de Trabalho. A definição da amostra não poderá ampliar os quantitativos máximos estabelecidos nesta seção sem formalização entre as partes.

13.2.6 A incorporação dos demais FQDNs e APIs ocorrerá conforme planejamento da CONTRATANTE, mediante os mecanismos operacionais regulares da solução. Serviços adicionais de implantação assistida ou customização poderão utilizar a consultoria especializada, mediante Ordem de Serviço.

13.3 Plano de Trabalho

13.3.1 Em até 5 dias úteis após a assinatura do contrato, será realizada reunião inicial entre a CONTRATANTE e a CONTRATADA para elaboração do Plano de Trabalho.

13.3.2 O Plano de Trabalho deverá conter, no mínimo:

- 13.3.2.1 equipes, responsáveis e pontos de contato;
- 13.3.2.2 cronograma, marcos e período de operação assistida;
- 13.3.2.3 arquitetura atual e proposta, incluindo pontos de inserção da solução;
- 13.3.2.4 FQDNs e APIs da amostra;
- 13.3.2.5 atividades e alterações necessárias em DNS, certificados, origens, cabeçalhos, firewall e health checks;
- 13.3.2.6 dependências, responsabilidades e janelas de mudança;
- 13.3.2.7 inventário e pesos dos serviços críticos para apuração da indisponibilidade parcial;
- 13.3.2.8 método de monitoramento e fontes de evidência da disponibilidade;
- 13.3.2.9 procedimentos de piloto, homologação, rollback e contingência;
- 13.3.2.10 documentação, evidências e entregáveis.

13.4 Documentação Técnica

- 13.4.1 A CONTRATADA deverá disponibilizar os manuais técnicos necessários à configuração e operação da solução, preferencialmente em português ou, quando indisponíveis, em inglês.

14. TREINAMENTO

- 14.1 A CONTRATADA deverá fornecer 6 vagas de treinamento oficial da solução, utilizáveis em até 3 turmas, agendas ou edições distintas, em até 180 dias contados da assinatura do contrato.
- 14.2 O cronograma deverá ser proposto pela CONTRATADA em até 20 dias corridos da assinatura e será definido em conjunto com a CONTRATANTE.
- 14.3 O treinamento deverá:
 - 14.3.1 ser ministrado em português;
 - 14.3.2 ser conduzido por instrutor qualificado pelo fabricante ou por centro de treinamento autorizado;
 - 14.3.3 contemplar conteúdo teórico e prático;
 - 14.3.4 abranger administração, configuração, operação, análise de eventos e resolução de problemas;
 - 14.3.5 fornecer material didático e acesso a ambiente de laboratório, quando previsto no curso oficial;
 - 14.3.6 assegurar a cada participante o conteúdo e a carga horária integral do curso correspondente;
 - 14.3.7 resultar na emissão de certificado de conclusão.
- 14.4 A carga horária corresponderá à carga oficial do treinamento aplicável à solução ofertada, sem exigência de adaptação ou ampliação do curso oficial pelo fabricante.
- 14.5 Serão aceitos vouchers para turmas abertas e treinamentos presenciais, remotos ou híbridos. A utilização das vagas em diferentes edições não poderá gerar cobrança adicional.
- 14.6 Quando a realização presencial fora do Município de São Paulo for determinada pela CONTRATADA, as despesas de deslocamento, hospedagem e alimentação dos participantes deverão estar incluídas no preço.
- 14.7 O prazo para realização poderá ser ajustado mediante acordo formal entre

as partes.

15. OBRIGAÇÕES DA CONTRATADA

15.1 A CONTRATADA deverá cumprir as obrigações estabelecidas neste Termo de Referência, em seus anexos e em sua proposta, assumindo os custos e os riscos necessários à adequada execução do objeto.

15.2 Compete à CONTRATADA:

15.2.1 disponibilizar e manter os recursos, capacidades, licenças, serviços e profissionais necessários;

15.2.2 cumprir os prazos, níveis de serviço e procedimentos de segurança e mudança;

15.2.3 corrigir falhas, vulnerabilidades e não conformidades sob sua responsabilidade;

15.2.4 manter atualizações, inteligência de ameaças, compatibilidade entre componentes e acesso ao suporte do fabricante;

15.2.5 preservar o sigilo e cumprir as obrigações de privacidade e proteção de dados;

15.2.6 elaborar, executar e manter atualizados os planos, documentos, registros e evidências previstos;

15.2.7 comunicar fatos que possam comprometer os prazos, a segurança ou a continuidade dos serviços;

15.2.8 prestar informações à gestão e fiscalização;

15.2.9 manter as condições de habilitação e cumprir as obrigações trabalhistas, fiscais, previdenciárias e comerciais.

15.3 A utilização de fabricante, provedor de nuvem, CDN, suboperador ou terceiro não afasta a responsabilidade integral da CONTRATADA.

15.4 Transição e Encerramento Contratual

15.4.1 Antes do término dos itens recorrentes ou em caso de rescisão, a CONTRATADA deverá:

15.4.1.1 fornecer o inventário de ativos, configurações, políticas customizadas e logs abrangidos pelo período de retenção, nos formatos disponíveis e, quando possível, em formato aberto ou legível;

15.4.1.2 entregar documentação atualizada da arquitetura e das configurações;

15.4.1.3 realizar a transferência de conhecimento;

15.4.1.4 remover acessos, credenciais e vínculos ativos;

15.4.1.5 eliminar com segurança os dados sob sua responsabilidade, fornecendo evidência quando solicitado.

15.4.2 Quando determinada configuração não puder ser exportada, deverá ser fornecida documentação suficiente para sua identificação e reconstrução. As atividades deverão começar com antecedência suficiente para sua conclusão antes da desativação da subscrição, sem impacto à continuidade operacional.

16. OBRIGAÇÕES DA CONTRATANTE

16.1 Compete à CONTRATANTE:

- 16.1.1 fornecer os acessos, informações, ativos e dados técnicos necessários;
- 16.1.2 disponibilizar os ativos selecionados para a amostra;
- 16.1.3 executar ou autorizar as alterações sob sua responsabilidade;
- 16.1.4 assegurar a participação das equipes necessárias;
- 16.1.5 analisar e aprovar planos, cronogramas, relatórios e evidências;
- 16.1.6 acompanhar e fiscalizar a execução;
- 16.1.7 comunicar falhas e impedimentos sob sua responsabilidade;
- 16.1.8 emitir os termos de aceite quando cumpridos os requisitos;
- 16.1.9 efetuar os pagamentos e retenções aplicáveis;
- 16.1.10 designar gestor e fiscal e manter os documentos da contratação.

16.2 A CONTRATANTE deverá comunicar tempestivamente os impedimentos sob sua responsabilidade que possam afetar o cronograma.

17. VISITA TÉCNICA

17.1 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.

17.2 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.

17.3 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.

17.4 Para agendamento e realização da visita, a LICITANTE, por seu representante legal ou representante devidamente autorizado, 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.

17.5 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: consultaseginform@prodam.sp.gov.br, devendo ser indicada, no ato da solicitação, a modalidade de visita pretendida (presencial ou remota).

17.6 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.

17.7 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 VI) 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.

17.8 A 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.

18. CONFIDENCIALIDADE

- 18.1 A CONTRATADA deverá preservar o sigilo das informações acessadas em razão do contrato, incluindo dados, sistemas, aplicações, infraestrutura, topologia, configurações, credenciais e eventos de segurança. As informações somente poderão ser utilizadas na execução do objeto e não poderão ser divulgadas ou compartilhadas, salvo quando necessário à prestação do serviço, autorizado pela CONTRATANTE ou exigido por lei.
- 18.2 O dever de confidencialidade permanecerá após o término do contrato. Todo acesso remoto ou intercâmbio de informações deverá utilizar mecanismo documentado, controlado, rastreável e compatível com as autorizações concedidas.
- 18.3 A CONTRATADA responderá pelas ações de seus empregados, representantes, fabricantes, suboperadores e demais terceiros envolvidos na prestação do serviço.

19. TRATAMENTO, RETENÇÃO E SOBERANIA DOS DADOS

- 19.1 A CONTRATADA deverá informar de forma clara e manter atualizados:
- 19.1.1 os locais de processamento do tráfego;
 - 19.1.2 os locais de armazenamento persistente de logs, metadados e eventos;
 - 19.1.3 os países e regiões utilizados para administração ou suporte;
 - 19.1.4 os suboperadores e as respectivas finalidades;
 - 19.1.5 os prazos de retenção;
 - 19.1.6 os mecanismos de eliminação segura.
- 19.2 É vedado o uso, compartilhamento ou retenção dos dados da CONTRATANTE para finalidade distinta da execução do objeto. Os dados coletados deverão permanecer sob seu controle e observar a LGPD e a legislação aplicável.
- 19.3 Os ambientes de armazenamento persistente deverão estar preferencialmente localizados no Brasil. O tratamento ou armazenamento de dados pessoais fora do território nacional dependerá de informação prévia, aprovação da CONTRATANTE e mecanismo válido de transferência internacional, observados os arts. 33 a 36 da LGPD e a regulamentação da ANPD.
- 19.4 Quando utilizadas cláusulas-padrão contratuais, deverão ser adotadas as cláusulas aprovadas pela ANPD, sem alterações incompatíveis com a regulamentação aplicável.

20. QUALIFICAÇÃO TÉCNICA

- 20.1 A licitante deverá apresentar um ou mais Atestados de Capacidade Técnica, emitidos por pessoa jurídica de direito público ou privado, em papel timbrado ou meio eletrônico institucional, devidamente identificados,

datados e assinados, contendo dados que permitam a identificação do emitente e comprovando experiência na implantação, operação e suporte de soluções WAF/WAAP prestadas em modelo SaaS, cloud-delivered ou serviço em nuvem compatível com a arquitetura do objeto.

20.2 Não será exigida identidade integral entre os quantitativos dos atestados e o Ambiente Estimado de Referência.

20.3 Os atestados deverão demonstrar experiência compatível em complexidade tecnológica e operacional, admitida a soma de atestados.

20.4 Não será exigida comprovação de marca ou fabricante específico nos atestados.

20.5 Caso a licitante não seja fabricante da solução ofertada, deverá apresentar declaração ou documento oficial emitido pelo fabricante comprovando que está autorizada a comercializar, implantar e prestar suporte da solução no Brasil. Serão aceitos documentos emitidos pelo fabricante previamente à publicação do edital, desde que válidos e compatíveis com a solução ofertada.

20.6 Para as comprovações que não constem de catálogos, folhetos, manuais e demais documentos técnicos, será aceita declaração do licitante, firmada por seu representante legal e sob as penas da lei, atestando que a solução ofertada cumpre as especificações exigidas, admitida também declaração do fabricante, dispensada destinação nominal e referência a este processo licitatório. A PRODAM-SP poderá realizar diligências junto ao fabricante para confirmar as informações prestadas, sujeitando o licitante às sanções cabíveis em caso de declaração falsa.

20.7 Formas de Comprovação dos Requisitos

20.7.1 Os requisitos técnicos serão comprovados pelas formas indicadas no Anexo VIII:

20.7.1.1 **DOC**: documentação oficial do fabricante, declaração formal da licitante ou do fabricante, proposta comercial, certificação, termo de serviço ou outra evidência tecnicamente adequada;

20.7.1.2 **DEM**: demonstração assistida no tenant da CONTRATANTE ou, quando não houver dados, histórico ou configurações suficientes, em ambiente demonstrativo do fabricante;

20.7.1.3 **HOM**: teste funcional realizado sobre FQDN ou API integrante da amostra.

20.7.2 DOC deverá acompanhar a proposta. DEM e HOM serão realizadas nas etapas indicadas neste Termo de Referência. O símbolo “+” indica a utilização combinada das formas de comprovação, limitada às parcelas descritas na coluna “Observações / expansão”, enquanto a expressão “ou” indica formas alternativas.

20.7.3 A proposta deverá identificar o produto, recurso, módulo, licença, capacidade, limite e mecanismo utilizados. Não será suficiente a indicação isolada “atende” ou “sim”, nem a simples reprodução do requisito.

20.7.4 DEM ou HOM não poderá ser utilizada para incluir posteriormente licença, módulo, capacidade ou funcionalidade ausente da proposta original.

20.7.5 Requisitos de capacidade global, arquitetura, escalabilidade, DDoS, alta disponibilidade, certificações, licenciamento e segurança do fabricante serão comprovados por DOC. Recursos administrativos,

inventários, relatórios, classificação automática e automação poderão utilizar DEM. HOM será limitada aos testes funcionais previstos para a amostra.

- 20.7.6 Não serão exigidos testes de carga ou saturação, reprodução das capacidades globais, ataques DDoS, falhas provocadas em PoPs, regiões ou infraestrutura compartilhada, geração artificial de volume de tráfego ou procedimentos que possam afetar aplicações em produção ou serviços de terceiros.

20.8 Matriz de Conformidade, Capacidade e Equivalência Técnica

- 20.8.1 A comprovação dos requisitos técnicos será consolidada na Matriz de Conformidade, Capacidade e Equivalência Técnica, constante do Anexo VIII.
- 20.8.2 A Matriz conterá os seguintes campos: I. identificação e grupo; II. requisito resumido; III. mínimo ou condição de atendimento; IV. oferta da licitante; V. inclusão; VI. forma de comprovação; VII. referência da evidência; e VIII. observações e condições de expansão, quando aplicáveis.
- 20.8.3 A CONTRATANTE preencherá previamente a identificação, o requisito resumido, o mínimo ou condição de atendimento, a forma de comprovação e as orientações específicas de expansão.
- 20.8.4 A licitante deverá preencher os campos relativos à oferta, inclusão, referência da evidência e observações ou condições de expansão.
- 20.8.5 Na oferta, a licitante deverá identificar objetivamente o recurso, módulo, licença, capacidade, franquia, limite ou mecanismo utilizado para atender ao requisito.
- 20.8.6 A simples indicação “atende”, “sim” ou a reprodução do requisito não será considerada descrição suficiente, salvo no campo específico de inclusão.
- 20.8.7 Para fins de análise da proposta técnica, os requisitos sujeitos a comprovação estão integralmente consolidados no Anexo VIII.
- 20.8.8 As demais disposições do Termo de Referência permanecem aplicáveis como obrigações de execução contratual, gestão, fiscalização, faturamento, aceite e encerramento, sem necessidade de comprovação individual na proposta, salvo indicação expressa em contrário.
- 20.8.9 Os preços de expansão serão solicitados somente para as capacidades identificadas na Matriz.
- 20.8.10 Quando a capacidade não for comercializada isoladamente, a licitante deverá informar o menor pacote, licença, plano ou combinação de recursos aplicável, com quantidade, periodicidade e preço.
- 20.8.11 A ausência de documentação pública não implicará desclassificação automática quando o requisito admitir declaração formal, demonstração ou diligência, observada a isonomia. Em caso de divergência entre a Matriz e a evidência, prevalecerá a capacidade comprovada. A ausência ou insuficiência de comprovação poderá ensejar diligência ou desclassificação, conforme a natureza e a obrigatoriedade do requisito.

21. ACEITE

21.1 Plano de Homologação e Critérios de Aprovação

21.1.1 A CONTRATADA deverá apresentar o Plano de Homologação e Testes em até 10 (dez) dias úteis após a assinatura do contrato, para análise e aprovação da CONTRATANTE.

21.1.2 O Plano de Homologação deverá conter, para cada teste:

- 21.1.2.1 requisito avaliado;
- 21.1.2.2 ativo da amostra utilizado;
- 21.1.2.3 procedimento resumido;
- 21.1.2.4 resultado esperado;
- 21.1.2.5 evidência;
- 21.1.2.6 situação: aprovado ou reprovado.

21.1.3 Os procedimentos poderão ser ajustados de comum acordo durante a implantação, desde que não reduzam os requisitos obrigatórios nem ampliem os quantitativos máximos da amostra.

21.1.4 Testes reprovados serão registrados como não conformidades e deverão conter ação corretiva, responsável e prazo para nova verificação.

21.1.5 O aceite dos Serviços de Implantação e Configuração será emitido após:

- 21.1.5.1 ativação do tenant, das contas, das licenças, dos módulos e das capacidades contratadas;
- 21.1.5.2 configuração e integração da solução;
- 21.1.5.3 entrada em produção da amostra definida no Plano de Trabalho;
- 21.1.5.4 aprovação dos testes obrigatórios aplicáveis à amostra;
- 21.1.5.5 conclusão da operação assistida;
- 21.1.5.6 entrega da documentação técnica;
- 21.1.5.7 apresentação dos documentos de riscos, privacidade e fluxo de dados;
- 21.1.5.8 correção das não conformidades impeditivas.

21.1.6 A homologação funcional será realizada exclusivamente sobre os FQDNs e APIs integrantes da amostra e contemplará:

- 21.1.6.1 I. encaminhamento e inspeção de tráfego HTTPS em pelo menos um FQDN;
- 21.1.6.2 II. ativação de uma regra WAF e verificação da ação configurada para uma requisição controlada;
- 21.1.6.3 III. preservação do IP de origem em pelo menos uma aplicação da amostra e, quando houver aplicação legada incompatível com o uso do mecanismo de preservação, demonstração da aplicação de política de segurança baseada no IP identificado pela plataforma;
- 21.1.6.4 IV. importação de especificação OpenAPI/Swagger e validação de requisição em relação ao schema, quando houver API e especificação disponíveis na amostra. Na ausência desses insumos, o teste será substituído por demonstração assistida com especificação de exemplo;
- 21.1.6.5 V. aplicação de uma regra de rate limiting ou de outra política específica por API, endpoint ou método HTTP;
- 21.1.6.6 VI. geração e envio de pelo menos um evento de segurança ao SIEM, SOAR ou destino indicado pela CONTRATANTE;
- 21.1.6.7 VII. autenticação administrativa com MFA e verificação de pelo menos dois perfis RBAC com permissões distintas;
- 21.1.6.8 VIII. validação do certificado utilizado por pelo menos um FQDN da amostra;
- 21.1.6.9 IX. rollback de uma alteração controlada de configuração;
- 21.1.6.10 X. avaliação funcional do impacto no desempenho, conforme a

subseção específica deste Termo de Referência.

- 21.1.7 O Plano de Homologação ficará restrito aos testes enumerados nesta seção, não podendo criar novos testes, ampliar a amostra ou converter requisitos documentais ou demonstrativos em testes funcionais, salvo acordo formal para esclarecimento de dúvida técnica específica.
- 21.1.8 Cada funcionalidade será verificada uma única vez em ativo tecnicamente adequado, sem necessidade de repetição em todos os FQDNs ou APIs, salvo reteste decorrente de não conformidade. Os demais requisitos serão comprovados conforme a Matriz de Conformidade.
- 21.1.9 Considera-se impeditiva a não conformidade que impossibilite o encaminhamento ou a proteção do tráfego, provoque indisponibilidade, erro recorrente ou bypass não autorizado, impeça funcionalidade submetida à homologação, comprometa a segurança, a privacidade ou a administração, demonstre ausência de recurso contratado ou inviabilize a integração mínima.
- 21.1.10 Não conformidades não impeditivas poderão ser registradas em plano de correção contendo ação, responsável e prazo aprovado pela CONTRATANTE, sem impedir a emissão do aceite. O prazo para correção das não conformidades não impeditivas será definido conforme sua natureza e complexidade e não deverá exceder 30 dias corridos contados da emissão do aceite, salvo justificativa técnica formalmente aprovada pela CONTRATANTE.
- 21.1.11 A emissão do aceite não afasta a obrigação de correção das pendências registradas nem implica renúncia aos demais requisitos contratuais.
- 21.1.12 A emissão do Termo de Aceite dos Serviços de Implantação e Configuração constituirá:
- 21.1.12.1 o marco para faturamento do item 2;
 - 21.1.12.2 o início dos 36 meses da subscrição, item 1;
 - 21.1.12.3 o início dos 36 meses do suporte técnico e sustentação, item 3;
 - 21.1.12.4 o início da apuração dos níveis de serviço dos itens recorrentes.
- 21.1.13 As não conformidades serão submetidas a nova verificação pelo mesmo meio de comprovação aplicável ao requisito, mediante documento corrigido, nova demonstração ou reteste funcional, sem ônus adicional.
- 21.1.14 A CONTRATANTE formalizará o aceite em até 3 dias úteis após a apresentação das evidências conclusivas, desde que não existam não conformidades impeditivas.
- 21.1.15 O faturamento observará as condições estabelecidas na seção CONDIÇÕES DE FATURAMENTO.
- 21.1.16 O aceite do treinamento será emitido em até 5 dias úteis após:
- 21.1.16.1 conclusão das vagas ou edições previstas;
 - 21.1.16.2 comprovação da carga horária e do conteúdo ministrado;
 - 21.1.16.3 entrega da relação de participantes;
 - 21.1.16.4 disponibilização dos certificados de conclusão.
- 21.1.17 Quando forem identificadas não conformidades, a CONTRATADA deverá corrigi-las ou disponibilizar nova oportunidade de treinamento, sem custo adicional.
- 21.1.18 Os certificados deverão ser emitidos em até 15 dias úteis após a conclusão do treinamento de cada participante.

22. CRITÉRIO DE JULGAMENTO E FORMAÇÃO DO VALOR GLOBAL

22.1 Para fins de julgamento e execução contratual, os itens 1 (Subscrição) e 3 (Suporte Técnico e Sustentação) serão considerados por 36 parcelas mensais.

22.2 O valor global de julgamento será calculado pela seguinte fórmula:

$$22.3 \text{ VG} = (\text{V1} \times 36) + \text{V2} + (\text{V3} \times 36) + (\text{V4} \times 6) + (\text{VH} \times 300)$$

22.4 Onde:

22.5 **VG**: valor global da proposta;

22.6 **V1**: valor mensal da subscrição;

22.7 **V2**: valor total do serviço de implantação;

22.8 **V3**: valor mensal do suporte;

22.9 **V4**: valor unitário por vaga de treinamento;

22.10 **VH**: valor unitário da hora de consultoria especializada.

22.11 Os valores relativos à consultoria serão considerados na formação do valor global para fins de julgamento, sem constituir obrigação de consumo ou pagamento integral pela CONTRATANTE.

23. CONDIÇÕES DE FATURAMENTO

23.1 Os itens 1 e 3 serão faturados mensalmente durante 36 meses a partir da emissão do Termo de Aceite dos Serviços de Implantação e Configuração. Não haverá faturamento recorrente antes desse marco.

23.2 O item 2 será faturado em parcela única após a emissão do respectivo Termo de Aceite, Anexo III.

23.3 O item 4 será faturado em parcela única após a conclusão e o aceite das seis vagas, mediante o Termo de Aceite de Recebimento do Treinamento, Anexo IV.

23.4 O item 5 será faturado por Ordem de Serviço, após o respectivo aceite, limitado às horas efetivamente executadas e aceitas.

23.5 A CONTRATADA deverá apresentar a decomposição mensal dos valores dos itens recorrentes, identificando a subscrição, o suporte e os módulos complementares, quando houver. A decomposição será utilizada para faturamento, reajuste, glosas e alterações contratuais, sem modificar o valor global, e deverá guardar coerência com a estrutura comercial e a relevância dos componentes, vedada a atribuição artificial, simbólica ou irrisória de valores.

24. CONDIÇÕES DE PAGAMENTO

24.1 A Nota Fiscal Eletrônica de Serviços deverá ser emitida e encaminhada à CONTRATANTE, por meio do setor de Expediente, para o endereço eletrônico gfl@prodam.sp.gov.br.

24.2 Após o recebimento da Nota Fiscal Eletrônica de Serviços, a CONTRATANTE disporá de até 5 (cinco) dias úteis para emissão do Termo de Aceite de Pagamento, aprovando os serviços prestados.

- 24.3 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.
- 24.4 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 5 (cinco) dias úteis. A devolução da Nota Fiscal Eletrônica de Serviços, devidamente regularizada pela CONTRATADA, deverá ser efetuada em até 5 (cinco) dias úteis da data de comunicação formal realizada pela CONTRATANTE.
- 24.5 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, 8 de setembro de 2026.

ALEXSANDER DE SOUZA

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\$
------	-----------	---------	------------	--------------------	-----------------

Item	Descrição	Unidade	Quantidade	Valor Unitário R\$	Valor Total R\$
1	Subscrição da solução Cloud WAF/WAAP por 36 meses, contados da emissão do Termo de Aceite dos Serviços de Implantação e Configuração, incluindo todas as licenças, módulos, capacidades, franquias, atualizações e demais recursos necessários ao atendimento integral do Ambiente Estimado de Referência.	Mês	36		
2	Serviço de implantação, configuração completa, integração e homologação inicial da solução Cloud WAF/WAAP, incluindo ativação do tenant, parametrização, piloto, implantação da amostra definida para aceite, operação assistida e entrega da documentação técnica.	Serviço	1		
3	Serviço continuado de suporte técnico e sustentação da solução Cloud WAF/WAAP por 36 meses, contados da emissão do Termo de Aceite dos Serviços de Implantação e Configuração.	Mês	36		
4	Treinamento oficial da solução, compreendendo 6 (seis) vagas, utilizáveis em até 3 (três) turmas, agendas ou edições distintas.	Vaga	6		
5	Consultoria Técnica Especializada sob demanda.	Hora técnica	300		

Preço Total (postado no sistema) por extenso.

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

OBSERVAÇÃO: Sobre o critério para formação do valor global da proposta ver explicações na seção **“CRITÉRIO DE JULGAMENTO E FORMAÇÃO DO VALOR GLOBAL”**.

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], executou os **Serviços de Implantação e Configuração da solução Cloud WAF/WAAP**, discriminados na documentação comprobatória da execução, 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.

EFEITOS DO ACEITE

A partir da data de emissão deste Termo:

1. Considera-se aceito o item 2, Serviço de Implantação e Configuração;
2. Inicia-se o período de 36 meses da subscrição da solução, item 1;
3. Inicia-se o período de 36 meses do suporte técnico e sustentação, item 3;
4. Inicia-se a apuração dos níveis de serviço dos itens recorrentes;
5. Fica autorizado o faturamento do item 2 e o início da medição mensal dos itens 1 e 3, nas condições estabelecidas no Termo de Referência.

Início dos itens recorrentes: ____/____/____

Término previsto dos itens recorrentes: ____/____/____

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 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], realizou o **treinamento oficial da solução Cloud WAF/WAAP**, conforme documentação comprobatória da execução constante do 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 - 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: _____

4. ESTIMATIVA DE ESFORÇO

Horas estimadas: _____

Valor da hora técnica: R\$ _____

Valor total estimado da OS: R\$ _____

5. PRAZO DE EXECUÇÃO

Data início: ____ / ____ / ____

Data conclusão: ____ / ____ / ____

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

6. ENTREGÁVEIS, CONFORME APLICÁVEL

() Plano de trabalho

() Relatório técnico

() Evidências de execução

() Configurações ou documentação atualizada

() Outro: _____

7. PREMISSAS E RESTRIÇÕES

Dependência de acesso ao ambiente

Aprovação prévia de mudanças críticas

Backup antes de alterações

8. ACEITE DA ESPECIFICAÇÃO

Pelo Prestador: _____

Assinatura: _____

Data: ____ / ____ / ____

9. FATURAMENTO E PAGAMENTO

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

O pagamento somente será efetuado após a emissão do Termo de Aceite da Ordem de Serviço de Consultoria, conforme o Anexo VII, caracterizando que a demanda foi atendida em perfeitas condições em relação às especificações e necessidades da PRODAM.

ANEXO VI - DECLARAÇÃO DE VISITA TÉCNICA

REF.: PREGÃO ELETRÔNICO NºXX.XXX/202_

ATESTO que o representante legal da 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.

A 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 VII - 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 à prestação dos **serviços de consultoria**, referentes à Ordem de Serviço nº [**inserir número**], emitida em / / 202_, conforme doc. SEI nº [**inserir o nº do doc. com hyperlink**], 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)

ANEXO VIII - MATRIZ DE CONFORMIDADE, CAPACIDADE E EQUIVALÊNCIA TÉCNICA

ID / Grupo	Requisito resumido	Mínimo ou condição de atendimento	Oferta da licitante	Inclusão	Comprovação	Referência da evidência	Observações / expansão
A1	Arquitetura Cloud/SaaS e segregação	Sem processamento nos datacenters da CONTRATANTE; segregação sem acesso cruzado.		SIM, incluído no preço / NÃO	DOC		Não requerida.

ID / Grupo	Requisito resumido	Mínimo ou condição de atendimento	Oferta da licitante	Inclusão	Comprovação	Referência da evidência	Observações / expansão
A2	Mitigação DDoS	Proteção L3/L4 na borda SaaS e L7 para os FQDNs protegidos, conforme o TR.		SIM, incluído no preço / NÃO	DOC		Não requerida.
A3	TLS	Suporte a TLS 1.2 e TLS 1.3.		SIM, incluído no preço / NÃO	DOC		Não requerida.
A4	Alta disponibilidade e continuidade	Redundância, recuperação automática, preservação de políticas e ausência de bypass.		SIM, incluído no preço / NÃO	DOC		Não requerida.
A5	Disponibilidade mensal	SLA mínimo de 99,95%.		SIM, incluído no preço / NÃO	DOC		Não requerida.
A6	Suporte técnico	Atendimento 24x7 em português, conforme os níveis de severidade do TR.		SIM, incluído no preço / NÃO	DOC		Não requerida.
B1	FQDNs protegidos	700 ativos e protegidos simultaneamente.		SIM, incluído no preço / NÃO	DOC		Informar preço por FQDN ou menor pacote para expansão até 1.050.
B2	APIs protegidas	100 APIs, sem limitação incompatível de endpoints, métodos ou versões.		SIM, incluído no preço / NÃO	DOC		Informar preço por API ou menor pacote para expansão até 150.
B3	Requisições processadas	7,78 bilhões por mês.		SIM, incluído no preço / NÃO	DOC		Informar preço por bilhão ou menor pacote para expansão até 11,67 bilhões/mês.
B4	RPS sustentado	3.000 RPS com as funções obrigatórias ativas.		SIM, incluído no preço / NÃO	DOC		Não requerida.
B5	RPS de pico	4.000 RPS.		SIM, incluído no preço / NÃO	DOC		Informar menor pacote para expansão até 6.000 RPS.

ID / Grupo	Requisito resumido	Mínimo ou condição de atendimento	Oferta da licitante	Inclusão	Comprovação	Referência da evidência	Observações / expansão
B6	Throughput sustentado	1,5 Gbps com as funções obrigatórias ativas.		SIM, incluído no preço / NÃO	DOC		Informar preço por Gbps ou menor pacote para expansão até 2,25 Gbps.
B7	Throughput de pico	3 Gbps.		SIM, incluído no preço / NÃO	DOC		Não requerida.
B8	Retenção de logs	30 dias.		SIM, incluído no preço / NÃO	DOC		Não requerida.
B9	Exportação de logs	1 TB por mês, incluindo processamento, transferência, egress e conectores.		SIM, incluído no preço / NÃO	DOC		Informar preço por TB ou menor pacote para expansão até 10 TB/mês.
B10	Espaços lógicos segregados	Múltiplos espaços com segregação, delegação e gestão centralizada.		SIM, incluído no preço / NÃO	DOC + DEM		Informar quantidade incluída ou "Ilimitado" e preço do menor pacote adicional.
C1	Proteção OWASP Top 10 Web	Proteção dos riscos tecnicamente tratáveis.		SIM, incluído no preço / NÃO	DOC + HOM		HOM limitada a uma regra WAF e uma requisição controlada.
C2	Proteção OWASP API Security Top 10	Mecanismos para os riscos tecnicamente tratáveis e controles para riscos de lógica.		SIM, incluído no preço / NÃO	DOC		Não requerida.
C3	Descoberta e inventário de APIs	Descoberta de APIs expostas, inclusive não documentadas ou desatualizadas, quando identificáveis.		SIM, incluído no preço / NÃO	DOC + DEM		Não requerida.
C4	OpenAPI e validação de schema	Importação OpenAPI/Swagger e validação de requisições em relação ao schema.		SIM, incluído no preço / NÃO	DOC + HOM		Sem especificação na amostra, substituir HOM por DEM com especificação de exemplo.

ID / Grupo	Requisito resumido	Mínimo ou condição de atendimento	Oferta da licitante	Inclusão	Comprovação	Referência da evidência	Observações / expansão
C5	Políticas por API, endpoint ou método	Criação de política específica e rate limiting ou controle equivalente.		SIM, incluído no preço / NÃO	DOC + HOM		HOM por uma regra de rate limiting ou política equivalente.
C6	Bot Management	Identificação, classificação e mitigação de bots e automações abusivas.		SIM, incluído no preço / NÃO	DOC + DEM		Não requerida.
C7	Preservação do IP e validação contra spoofing	Preservação do IP original e validação contra spoofing; política na camada WAAP para legado.		SIM, incluído no preço / NÃO	DOC + HOM		HOM do IP em uma aplicação; validação contra spoofing por DOC ou DEM.
C8	Inteligência de ameaças e virtual patching	Inteligência atualizada e mitigação de vulnerabilidades conhecidas.		SIM, incluído no preço / NÃO	DOC		Não requerida.
D1	Integração SIEM/SOAR	Syslog, CEF, LEEF, API ou equivalente, em tempo próximo ao real.		SIM, incluído no preço / NÃO	DOC + HOM		HOM mediante envio de pelo menos um evento ao destino indicado.
D2	Recuperação de eventos	Reenvio, recuperação ou nova consulta após indisponibilidade temporária do destino.		SIM, incluído no preço / NÃO	DOC ou DEM		Não requerida.
D3	Certificados digitais	Emissão, renovação automática, inventário, BYOC, proteção de chaves e auditoria.		SIM, incluído no preço / NÃO	DOC + DEM + HOM		HOM limitada ao certificado de um FQDN. As demais funções serão comprovadas por DOC ou, quando necessário, por DEM.
D4	Administração segura	MFA, RBAC, SSO por SAML ou OIDC e trilhas de auditoria.		SIM, incluído no preço / NÃO	DOC + DEM + HOM		HOM limitada a MFA e dois perfis RBAC. SSO, auditoria e demais mecanismos serão comprovados por DOC ou, quando necessário, por DEM.

ID / Grupo	Requisito resumido	Mínimo ou condição de atendimento	Oferta da licitante	Inclusão	Comprovação	Referência da evidência	Observações / expansão
D5	APIs de administração e automação	APIs oficialmente suportadas para administração e automação.		SIM, incluído no preço / NÃO	DOC + DEM		Não requerida.
E1	Privacidade, localização e transferência de dados	Atendimento à LGPD e às condições de localização, retenção, suboperadores e transferência internacional.		SIM, incluído no preço / NÃO	DOC		Informar locais de processamento de tráfego, armazenamento persistente, países ou regiões de administração e suporte e suboperadores envolvidos.
E2	Segurança do fabricante e cadeia de suprimentos	Política de vulnerabilidades, advisories/CVEs, atualizações e certificação exigida no TR.		SIM, incluído no preço / NÃO	DOC		Não requerida.
F1	Proteção específica para GraphQL	Recurso adicional de proteção para APIs GraphQL.		Ofertado opcionalmente / NÃO	DOC		O não atendimento não implica desclassificação.
F2	gRPC	Suporte adicional a gRPC.		Ofertado opcionalmente / NÃO	DOC		O não atendimento não implica desclassificação.
F3	CI/CD e infraestrutura como código	Integrações adicionais com CI/CD e IaC.		Ofertado opcionalmente / NÃO	DOC		O não atendimento não implica desclassificação.
F4	GSLB e balanceamento global	Recurso adicional de GSLB ou balanceamento global.		Ofertado opcionalmente / NÃO	DOC		O não atendimento não implica desclassificação.

ORIENTAÇÕES PARA PREENCHIMENTO DA MATRIZ (ANEXO VIII)

1. A licitante deverá preencher todos os campos a ela destinados.
2. A coluna "Oferta da licitante" deverá identificar objetivamente a capacidade, funcionalidade, licença, módulo, franquia, limite ou mecanismo de atendimento.
3. Não será aceita, isoladamente, a reprodução do requisito ou a indicação genérica "atende".
4. Para requisito obrigatório, a coluna "Inclusão" deverá conter "SIM, incluído no preço" ou "NÃO". A resposta "PARCIAL" não será admitida. Quando houver mecanismo alternativo ou equivalência, deverá ser indicado "SIM, incluído no preço" e o mecanismo será descrito na oferta.

- 5 . Para requisito opcional, a coluna “Inclusão” deverá conter “Ofertado opcionalmente” ou “NÃO”. O não atendimento não implicará desclassificação.
6. A coluna “Referência da evidência” deverá indicar o nome do documento, página e seção. Link eletrônico poderá ser apresentado complementarmente.
7. O símbolo “+” indica a utilização combinada das formas de comprovação, limitada às parcelas expressamente descritas na coluna “Observações / expansão”.
8. DOC deverá ser apresentado com a proposta. DEM e HOM serão realizadas nas etapas indicadas no Termo de Referência.
9. Quando a HOM depender de ativo ou insumo da CONTRATANTE indisponível, será aplicada a forma alternativa expressamente prevista na linha.
10. DEM ou HOM não poderá incluir posteriormente licença, módulo, capacidade ou funcionalidade ausente da proposta original.
11. Em divergência entre a Matriz e a evidência, prevalecerá a capacidade comprovada, sem prejuízo de diligência.
12. Preços de expansão serão apresentados somente nas linhas que os solicitarem. Se a expansão não for comercializada isoladamente, informar o menor pacote aplicável, sua quantidade, periodicidade e preço.
13. As linhas A a E consolidam os requisitos técnicos obrigatórios sujeitos a comprovação na proposta. O Grupo F possui caráter informativo e opcional. As demais disposições do TR permanecem como obrigações contratuais.



Allexsander de Souza
Gerente

Em 09/09/2026, às 12:17.

A autenticidade deste documento pode ser conferida no site
<http://processos.prefeitura.sp.gov.br>, informando o código verificador **164609354** e o código CRC **5DFA126F**.

V13.1

Referência: Processo nº 7010.2026/0005768-5

SEI nº 164609354