Especificação Técnica

TR Aquisição de Serviço de Proteção Anti-DDoS Baseado em Nuvem
Elaborado Exclusivamente para a PROCEMPA junto ao SEI 26.12.000000028-3
Validade: de 21/08/2026 a 21/02/2027

Requisitos Técnicos

TERMO de REFERÊNCIA

AQUISIÇÃO DE SERVIÇO DE PROTEÇÃO ANTI-DDOS BASEADO EM NUVEM (CLOUD)

OBJETO

Contratação de serviço especializado de proteção contra-ataques de Negação de Serviço Distribuído (DdoS) e outros ataques a partir da internet, baseado em nuvem, para garantia da continuidade, disponibilidade e integridade dos serviços de TI prestados pela Procempa à Prefeitura Municipal de Porto Alegre.

1. SUMÁRIO EXECUTIVO

A Procempa, como principal provedora de serviços de tecnologia da informação e comunicação para a Prefeitura de Porto Alegre, necessita proteger sua infraestrutura crítica contra ameaças cibernéticas modernas, em especial ataques de DDoS. Estes ataques podem tornar serviços essenciais indisponíveis para a população, causando prejuízos operacionais, financeiros e de imagem.

Este Termo de Referência visa a contratação de uma solução robusta, escalável e de classe mundial, baseada em uma rede global de proteção, capaz de mitigar ataques de qualquer escala sem impactar a experiência do usuário final.

2. OBJETO DA CONTRATAÇÃO

Contratação de serviço de proteção Anti-DDoS baseado em nuvem, do tipo **Sempre Ativo (Always-On),** incluindo:

2.1. **Proteção de Infraestrutura (Camadas 3 e 4 do modelo OSI**): Mitigação em linha de ataques volumétricos e de protocolo.
2.2. **Proteção de Aplicações (Camada 7 do modelo OSI**): Mitigação de ataques de exaustão de recursos e ataques complexos direcionados a aplicações web e APIs.
2.3. **Serviço de Web Application Firewall (WAF)** Integrado e gerenciável.
2.4. **Serviço de DNS Autoritativo** com proteção integrada contra-ataques.
2.5. Suporte Técnico Especializado 24x7x365.
2.6. Capacitação e atualização técnica
2.7. **Plataforma de Relatórios e Analytics** em tempo real.

3. JUSTIFICATIVA

A infraestrutura da Procempa é de missão crítica, suportando sistemas de saúde, educação, finanças e serviços ao cidadão. Ataques DDoS modernos superam a capacidade de links de internet e de soluções on-premise. A contratação de um serviço em nuvem, com uma rede global de scrubbing e roteamento anycast, é a única forma eficaz de mitigar ataques de grande escala, assegurando a resiliência e a continuidade dos serviços públicos.

Especificação Técnica

TR Aquisição de Serviço de Proteção Anti-DDoS Baseado em Nuvem
Elaborado Exclusivamente para a PROCEMPA junto ao SEI 26.12.000000028-3
Validade: de 21/08/2026 a 21/02/2027

4. ESPECIFICAÇÕES TÉCNICAS MÍNIMAS OBRIGATÓRIAS

O licitante deverá comprovar o atendimento aos seguintes requisitos:

4.1. Caracterização do Ambiente a Ser Protegido

Os quantitativos a seguir descrevem a configuração atual do ambiente da Procempa e destinam-se ao dimensionamento das propostas. Trata-se de referência de porte, sujeita a variação ao longo da vigência contratual, não constituindo limite rígido para a prestação do serviço.

4.1.1. Proteção de Infraestrutura (Camadas 3 e 4)

Blocos de endereçamento IP a serem protegidos:

- 4.1.1.1. 200.169.16.0/20
- 4.1.1.2. 201.7.128.0/20
- 4.1.1.3. 187.110.192.0/20
- 4.1.1.4. 2804:f4::/32

Banda de tráfego legítimo que deverá ser entregue limpa ao datacenter da Procempa após a mitigação: aproximadamente 500 Mbps destinados à DMZ (conexões externas às aplicações).

4.1.2. Proteção de Aplicações (Camada 7):

Aproximadamente 40 (quarenta) domínios, totalizando cerca de 760 (setecentos e sessenta) subdomínios/FQDNs, quantitativo que varia ao longo do tempo.
Volume mensal aproximado de 35 TB (trinta e cinco terabytes) de tráfego em requisições HTTP/HTTPS.

4.1.3. Web Application Firewall (WAF):

A política de WAF deverá cobrir aproximadamente 40 (quarenta) zonas DNS.
Serão utilizados certificados TLS próprios da Procempa, não sendo objeto desta contratação o fornecimento ou a gestão de certificados digitais; a solução deverá permitir a importação e a atualização desses certificados pela própria Procempa.

4.1.4. Serviço de DNS Autoritativo:

Deverão ser hospedadas 7 (sete) zonas DNS no serviço autoritativo protegido.
A Procempa não estabelece volume mínimo de consultas; exige-se, contudo, que a proteção e a resolução não sofram interrupção, degradação ou restrição em decorrência de picos de consultas legítimas.

4.1.5. Relatórios, Registros (Logs) e Integração:

Retenção mínima de 30 (trinta) dias dos registros de tráfego, de ataques e de eventos de WAF, com recurso de exportação disponível à Procempa.
Disponibilização de API RESTful, em padrão aberto, que permita a integração dos registros e métricas com qualquer ferramenta de SIEM ou de análise adotada pela Procempa.

4.2. Arquitetura e Capacidade da Rede de Mitigação

4.2.1. Rede global própria e dedicada à mitigação de DDoS, com capacidade agregada de scrubbing mínima de **20 Tbps**.

4.2.2. No mínimo, **10** Pontos de Presença (PoPs) de entrega de conteúdos distribuídos **em território nacional (Brasil) e em outros países da América do Sul**, com suporte a roteamento anycast para o serviço, devendo contar com pelo menos **5 PoPs localizados no território brasileiro**.

4.2.3. Ao menos **1 (um)** PoP que funciona como centro de mitigação (scrubbing center) com capacidade de mitigação simultânea nos níveis L3, L4 e L7, localizado em território brasileiro.

4.2.4. Infraestrutura da contratada (PoPs) presente em **no mínimo 100 países**, assegurando atuação mundial com distribuição de tráfego e mitigação próxima à origem dos ataques.

4.2.5. Possuir PoPs operacionais em **pelo menos 5 continentes**, garantindo capacidade de mitigação distribuída globalmente.

4.2.6. Os PoPs deverão operar de forma **redundante** e independente, assegurando continuidade do serviço por meio de **fail-over automático entre regiões geográficas distintas**.

4.2.7. Garantia contratual de disponibilidade do serviço superior a 99,99%.

4.3. Funcionalidades de Mitigação

4.3.1. Proteção de Infraestrutura (L3/L4)

4.3.1.1. Mitigação automática e em linha (sem necessidade de acionamento manual) para ataques como SYN/ACK Floods, UDP Floods, ICMP Floods, DNS e NTP Amplification, entre outros.

4.3.1.2. Análise comportamental do tráfego em tempo real para identificação de anomalias.

4.3.2. Proteção de Aplicações (L7)

4.3.2.1. Mitigação de ataques HTTP/HTTPS Floods, ataques de força bruta (como em páginas de login), Slowloris, Slow POST, e ataques direcionados a APIs.

4.3.2.2. Capacidade de criar regras personalizadas e de taxa (rate limiting) para proteger endpoints específicos.

4.3.3. Web Application Firewall (WAF)

4.3.3.1. Motor de assinaturas atualizado automaticamente para proteção contra as vulnerabilidades do OWASP Top 10 e CVEs pertinentes.

4.3.3.2. Interface para criação de regras personalizadas de segurança (Allowlist, Blocklist, Regras baseadas em SQLi, XSS, etc.), disponível para a Procempa.

4.3.3.3. Mitigação de tentativas de exploração de vulnerabilidades desconhecidas e ainda sem assinatura publicada, mediante modelos de inteligência artificial e/ou aprendizado de máquina.

4.3.4. Serviço de DNS

4.3.4.1. Serviço de DNS autoritativo global com proteção nativa contra-ataques de envenenamento de cache, amplificação e exaustão de recursos.

4.4. Requisitos de Desempenho e Integração

4.4.1. A solução não deve adicionar uma latência perceptível ao tráfego legítimo, com um acréscimo máximo de **50 ms** (medido do usuário final até a origem), em condições normais.

4.4.2. O serviço deverá oferecer tempo médio de **detecção** inferior ou igual a **5 segundos**, considerando a identificação automática do ataque e o acionamento do mecanismo de mitigação.

4.4.3. Tempo de **Mitigação** (TTM - Time to Mitigate) automático inferior a **10 segundos** a partir da detecção do ataque.

4.4.4. Fornecimento de uma **API RESTful** completa para integração com sistemas internos de segurança (ex.: SIEM) e automação de processos.

4.4.5. Portal de gestão centralizado (dashboard) com visualização em tempo real de ameaças, tráfego, relatórios de ataques e configurações de segurança.

4.5. Suporte e Gestão da Conta:

4.5.1. Suporte técnico especializado em segurança, disponível **24x7x365**, por telefone e portal próprio, com tempo de resposta máximo de **15 minutos** para incidentes críticos (interrupção de serviço).

4.5.2. Atribuição de um **Engenheiro de Conta ou Customer Success Manager** como ponto focal estratégico.

4.6. Capacitação da equipe Procempa

Treinamento de Implantação

4.6.1. A contratada deverá ministrar treinamento técnico presencial à equipe da Procempa, com carga horária mínima de **24 horas-aula**, para até 2 turmas de **no máximo 8 participantes cada**, em até **60** dias após a assinatura do contrato.

4.6.2. O conteúdo programático mínimo deverá abranger:

4.6.2.1. Ataques volumétricos e de protocolo (L3/L4): inundações por banda e por pacotes, esgotamento de estado (SYN/ACK flood), reflexão e amplificação (DNS, NTP, CLDAP, SSDP, Memcached, QUIC), ataques a DNS (NXDOMAIN e random subdomain), carpet bombing, pulse wave e ataques multivetor de curta duração;

4.6.2.2. Ataques à camada de aplicação (L7): HTTP flood com cache-busting, ataques a endpoints de alto custo, técnicas low and slow (Slowloris, Slow POST), vetores específicos de HTTP/2 e HTTP/3 (HTTP/2 Rapid Reset, CONTINUATION Flood, MadeYouReset), exaustão de handshake TLS, abuso de APIs, ataques algorítmicos (ReDoS) e abuso por tráfego automatizado conforme a taxonomia OWASP Automated Threats (OAT), incluindo credential stuffing e scraping, suas técnicas de detecção e de evasão;

4.6.2.3. WAF: modelos de detecção positiva e negativa, conjuntos de regras gerenciadas (OWASP Core Rule Set, níveis de paranoia e pontuação de anomalia), regras customizadas, rate limiting, virtual patching e tratamento de falsos positivos, aplicados às vulnerabilidades do OWASP Top 10 e do OWASP API Security Top 10 vigentes, bem como técnicas de evasão e limitações do controle, incluindo a proteção do endereço de origem;

4.6.2.4. Arquitetura de mitigação: always-on versus on-demand, redes anycast e centros de depuração, desvio por BGP, RTBH e Flowspec, controles de taxa e de identidade, resiliência da aplicação e degradação graciosa;

4.6.2.5. Detecção e operação: construção de linha de base, telemetria e interpretação de painéis, integração com SIEM, runbook de resposta a incidente, escalonamento ao suporte do fabricante e simulação controlada de ataque.

Cada tema deverá ser apresentado em sua fundamentação conceitual e, em seguida, em sua aplicação na plataforma contratada, vedado conteúdo de natureza comercial ou restrito somente à demonstração de funcionalidades.

4.6.3. Atualização Técnica e Intercâmbio Profissional:

4.6.3.1. Em cada ciclo anual do contrato, a contar a partir da data de sua assinatura, A CONTRATADA deverá disponibilizar anualmente 02 (dois) vagas para colaboradores do CONTRATANTE para a participação em, no mínimo, 1 (um) evento nacional e 1 (um) evento internacional de tecnologia promovidos pelo fabricante da solução ou dos quais o fabricante participe, com conteúdo técnico ou científico relacionado ao objeto deste edital.

4.6.3.2. É vedado o oferecimento de eventos de caráter exclusivamente comercial, promocional ou de lançamento de produtos, devendo cada evento promover atualização técnica e intercâmbio profissional com especialistas do fabricante, com a comunidade técnica da área e com outras organizações usuárias de serviço igual ou semelhante ao objeto deste edital.

4.6.3.3. Correrão por conta da CONTRATADA as despesas de inscrição e credenciamento e, quando o evento ocorrer fora de Porto Alegre, também as de transporte aéreo e local, hospedagem e alimentação dos participantes indicados.

4.7. Conformidade e Segurança:

4.7.1. O fabricante da solução deverá possuir certificações de segurança válidas, incluindo, mas não se limitando a, **ISO 27001 e SOC 2 Type II**.

4.7.2. A contratada e o fabricante da solução deverão assegurar a **confidencialidade integral** de todos os dados, registros, relatórios e incidentes relacionados à contratante, em conformidade com a **Lei nº 13.709/2018 (LGPD)** e com normas reconhecidas de segurança da informação, especialmente as **ISO/IEC 27001, ISO/IEC 27002** e suas extensões ou equivalentes.

A **comprovação da conformidade** deverá ser feita por meio de **evidências documentais** que demonstrem a implementação efetiva de controles, políticas e práticas de segurança da informação, incluindo, no mínimo:

4.7.2.1. Política de Segurança da Informação e Política de Privacidade Corporativa vigentes;

4.7.2.2. Procedimentos formais de controle de acesso, criptografia, registro e auditoria;

4.7.2.3. Declaração de conformidade à LGPD, assinada pelo Encarregado de Proteção de Dados (DPO), descrevendo as medidas técnicas e administrativas adotadas para a proteção dos dados pessoais e corporativos tratados no âmbito do serviço.

Especificação Técnica

TR Aquisição de Serviço de Proteção Anti-DDoS Baseado em Nuvem
Elaborado Exclusivamente para a PROCEMPA junto ao SEI 26.12.000000028-3
Validade: de 21/08/2026 a 21/02/2027

5. METODOLOGIA DE IMPLANTAÇÃO E MIGRAÇÃO

O licitante deverá apresentar um Cronograma Detalhado de Implantação que inclua, no mínimo:

5.1. **Kick-off e Descoberta**: Alinhamento de expectativas e detalhamento da arquitetura de rede atual da Procempa.

5.2. **Configuração e Testes em Sandbox**: Configuração inicial das políticas de segurança, WAF e DNS em um ambiente de testes.

5.3. **Migração Faseada**: Plano detalhado para migração do tráfego (IPs e domínios) de forma controlada, com um plano de rollback claro para cada fase.

5.4. **Testes de Validação**: Realização de testes de penetração controlados e simulações de ataque, coordenados com a equipe da Procempa, para validar a eficácia da mitigação.

5.5. **Go-Live e Otimização Contínua**: Transição para operação assistida e revisões periódicas de performance e segurança.

6. CRITÉRIOS DE AVALIAÇÃO E JULGAMENTO

O julgamento das propostas será realizado pelo **critério de MENOR PREÇO GLOBAL, desde que atendidas integralmente as especificações técnicas mínimas obrigatórias** estabelecidas no item 4 neste Termo de Referência.

7. DOCUMENTAÇÃO EXIGIDA

7.1. Proposta Comercial e Proposta Técnica detalhadas.

7.2. Documentação legal (Contrato Social, Certidões).

7.3. Certificados de conformidade (ISO, SOC2).

7.4. Política de Privacidade e Tratamento de Dados compatível com a LGPD.

7.5. Relatório ou Case Study de pelo menos 2 (duas) implementações de sucesso com porte similar.

8. VIGÊNCIA DO CONTRATO

8.1. Vigência de 36 (trinta e seis) meses, com cláusula de prorrogação por até 24 (vinte e quatro) meses adicionais, a critério da Procempa.