GOVERNO DO ESTADO DE MINAS GERAIS

Secretaria de Estado de Fazenda

Divisão de Segurança da Informação

Estudo Técnico Preliminar (ETP) 112396591 - SEF/STI-GOVERNANÇA-DSI

Belo Horizonte, 28 de abril de 2025.

ESTUDO TÉCNICO PRELIMINAR

1. INFORMAÇÕES GERAIS

1.1. Identificação do processo e solicitante

1.1.1. **Número do processo SEI:** 1190.01.0006603/2025-21

1.1.2. **Área solicitante:** SEF/STI-DGV.

1.1.3. **Objeto da contratação:** contratação de Plataforma Segura para Acesso à Internet, com funcionalidades como Web Application and API Protection (WAAP), Rede de Entrega de Conteúdo (CDN), Gerenciamento de DNS, Web Application Firewall (WAF), Anti-DDoS, Proteção de DNS, Zero Trust, SSE (Secure Service Edge) e outras funcionalidades de segurança e performance, visando proteger a infraestrutura digital da Secretaria de Estado de Fazenda de Minas Gerais (SEF/MG) e garantir a segurança e a performance do acesso aos serviços online disponibilizados pelo órgão, bem como a contratação de serviços de instalação, configuração e testes, suporte e treinamento por um período de 12 (doze) meses.

1.2. Equipe de Planejamento da Contratação (SEI)

Área solicitante e técnica*: Daniel de Oliveira Rezende - Masp 669.570-4 (titular) e Luciano Marques Viana - Masp 669.700-7 (suplente);

Equipe de contratação (planejamento): Cléia Mendes Ferreira – Masp: 752.494-5 (titular) e Paulo Henrique Macedo Vale – Masp: 669.628-0 (suplente);

Autoridade Competente: Rogério Zupo Braga – Masp: 668.359-3.

* A equipe técnica solicitou esta contratação, portanto, o mesmo representante da equipe técnica é também responsável pela solicitação.

Esta equipe de planejamento da contratação não vislumbrou necessidade de classificação desse estudo segundo a Lei de Acesso à Informação, Lei nº 12.527/2011, pois não está presente nenhuma das hipóteses previstas no art. 23 da referida lei, que ensejaria restrições à divulgação ou acesso às informações nele constantes.

2. DIAGNÓSTICO DA SITUAÇÃO ATUAL

2.1. Descrição do problema a ser resolvido ou da necessidade apresentada (art. 6º, I e IV)

Atualmente, as equipes responsáveis por gerir a infraestrutura digital da SEF/MG enfrentam os seguintes desafios:

- Os serviços online da secretaria estão expostos a diversas ameaças cibernéticas, incluindo ataques

de negação de serviço distribuído (DDoS), explorações de vulnerabilidades em aplicações web (OWASP Top 10), injeções de SQL, cross-site scripting (XSS) e outras tentativas de invasão e interrupção dos serviços. A ausência de estrutura de proteção em camadas aumenta o risco de indisponibilidade, perda de dados, comprometimento da reputação e potenciais prejuízos financeiros.

- O tempo de carregamento das páginas e a latência no acesso aos serviços online podem impactar negativamente a experiência do usuário, levando à frustração e, consequentemente, prejuízos à SEF/MG, seja em termos de produtividade interna, interação com os cidadãos/contribuintes ou acesso aos serviços públicos fornecidos.
- A ausência de recursos adequados para monitorar e gerenciar o tráfego de internet dificulta a identificação de ameaças em tempo real, a análise de padrões de acesso e a implementação de políticas de segurança consistentes.
- Com o crescimento da infraestrutura da SEF/MG, o aumento da complexidade e do volume de tráfego online, torna-se crucial contar com soluções que possam escalar de forma eficiente para atender às demandas futuras sem comprometer a segurança e a performance.
- As VPNs foram desenvolvidas para uma era em que os usuários se conectavam remotamente ao data center corporativo, porém, com o passar do tempo, tornaram-se um gargalo de segurança e produtividade pelos seguintes motivos: superfície de ataque ampla, falta de visibilidade e controle granular, desempenho e experiência do usuário degradados, vulnerabilidades e gestão complexa e confiança cega e inadequação à nuvem, pois o modelo de VPN é baseado na premissa ultrapassada do ponto de vista de segurança que é confiar em qualquer usuário que consiga se autenticar.
- A Secretaria está sujeita a uma série de regulamentações específicas de proteção de dados e segurança da informação (a exemplo do Sigilo Fiscal e da Lei Geral de Proteção de Dados Pessoais), tornando a implementação de medidas de segurança robustas uma necessidade para garantir a conformidade legal.

2.2. Justificativa do Quantitativo da Contratação

O quantitativo da contratação será determinado com base nos seguintes fatores:

- **Volume de tráfego:** A estimativa do tráfego de dados mensal e o pico de tráfego esperado nos serviços online da SEF/MG.
- **Número de domínios e subdomínios:** A quantidade de domínios e subdomínios que necessitam de proteção e otimização.
- **Número de aplicações web:** A quantidade de aplicações web que serão protegidas.
- **Requisitos de largura de banda:** A largura de banda necessária para garantir a performance dos serviços online sob diferentes condições de tráfego.
- **Funcionalidades específicas:** As funcionalidades específicas que são essenciais para atender às necessidades de segurança e performance da secretaria, como Web Application Firewall, mitigação avançada de DDoS, funcionalidades de CDN (caching, compressão, entre outras), análise de segurança e geração de relatórios.
- **Número de usuários:** Em alguns casos, o modelo de precificação pode considerar o número de usuários que acessam os serviços protegidos.

O dimensionamento preciso será realizado durante a fase de prospecção de soluções, considerando as ofertas dos diferentes fornecedores e as características específicas de cada plataforma.

2.3. Alinhamento entre a contratação e o planejamento da Administração (art. 6º, II)

A contratação da Plataforma Segura para Acesso à Internet está alinhada ao planejamento estratégico da Superintendência de Tecnologia da Informação (STI) nos seguintes aspectos:

- A iniciativa reforça a política de segurança da informação da SEF/MG, protegendo os ativos digitais e garantindo a continuidade dos serviços.

- A Plataforma Segura para Acesso à Internet contribui para a modernização da infraestrutura tecnológica, otimizando a performance dos serviços online e melhorando a experiência do usuário, elementos chave na jornada de transformação digital.
- Ao automatizar a proteção contra ameaças e otimizar a entrega de conteúdo, a Plataforma Segura para Acesso à Internet pode reduzir a carga sobre as equipes de TI, permitindo que se concentrem em outras atividades estratégicas.
- A proteção contra ataques DDoS e outras interrupções garante a disponibilidade dos serviços online, um fator crítico para a continuidade dos negócios da secretaria.
- A Plataforma Segura para Acesso à Internet pode auxiliar no cumprimento de regulamentações e padrões de segurança, fortalecendo a governança da informação.

A contratação das soluções de Web Application e API Protection e Security Service Edge, prevista no Orçamento Base Zero 2025, são imprescindíveis ao processo de aperfeiçoamento da postura de segurança da informação na SEF/MG, com foco no desenvolvimento de ações inerentes à proteção e privacidade dos dados e à garantia de confidencialidade, integridade e disponibilidade dos sistemas/aplicações e das informações tratadas no âmbito desta Secretaria. Importante destacar que esta despesa encontra-se programada dentro do planejamento anual de compras desta unidade e está acobertada pelas dotações orçamentárias 1191.04.126.033.2006.0001.3390.4002 e 1191 04 126 033 2006 0001 3390 3953, fontes 10.1 e /ou 29.1.

2.4. Descrição dos requisitos da potencial contratação (art. 6º, III)

As soluções a serem contratadas deverão atender aos seguintes requisitos mínimos:

2.4.1. Funcionalidades de Segurança

2.4.1.1. Firewall de Aplicação Web (WAF) com regras personalizáveis e proteção contra as vulnerabilidades do OWASP Top 10.

2.4.1.2. Proteção contra ataques de negação de serviço distribuído (DDoS) em diferentes camadas (rede, transporte e aplicação).

2.4.1.3. Mitigação de bots maliciosos e prevenção de fraudes.

2.4.1.4. Gerenciamento de certificados SSL/TLS.

2.4.1.5. Possibilidade de implementação de políticas de segurança personalizadas.

2.4.1.6. Registro e análise de logs de segurança.

2.4.1.7. Zero Trust Network Access.

2.4.1.8. Secure Web Gateway.

2.4.1.9. Cloud Access Security Broker.

2.4.1.10. Data Loss Prevention

2.4.2. Funcionalidades de Performance

2.4.2.1. Rede de Entrega de Conteúdo (CDN) com ampla distribuição geográfica de servidores.

2.4.2.2. Caching de conteúdo estático e dinâmico.

2.4.2.3. Otimização de imagens e outros recursos.

2.4.2.4. Compressão de dados.

2.4.2.5. Balanceamento de carga (load balancing).

2.4.3. Gerenciamento e Monitoramento

2.4.3.1. Painel de controle intuitivo e de fácil utilização.

2.4.3.2. Monitoramento em tempo real do tráfego e das ameaças.

2.4.3.3. Geração de relatórios detalhados sobre segurança e performance.

2.4.3.4. APIs para integração com outras ferramentas de segurança e monitoramento.

2.4.4. Confiabilidade e Disponibilidade

2.4.4.1. Acordo de Nível de Serviço (SLA) que garanta alta disponibilidade da plataforma.

2.4.4.2. Infraestrutura robusta e redundante.

2.4.5. Suporte Técnico

2.4.5.1. Suporte técnico especializado e responsivo.

2.4.5.2. Documentação clara e abrangente.

2.4.6. Escalabilidade

2.4.6.1. Capacidade de escalar os recursos de acordo com o crescimento da demanda.

2.4.7. Conformidade

2.4.7.1. Atendimento a padrões e regulamentações de segurança relevantes para a SEF/MG.

2.4.8. Integração

2.4.8.1. Facilidade de integração com a infraestrutura existente da Secretaria.

As Plataformas para Acesso Seguro à Internet oferecem uma ampla gama de funcionalidades que permitirão à SEF/MG proteger a infraestrutura digital da Secretaria de Estado de Fazenda de Minas Gerais (SEF/MG) e garantir a segurança e a performance do acesso aos serviços online disponibilizados pelo órgão.

3. PROSPECÇÃO DE SOLUÇÕES

3.1. Levantamento de Mercado (art. 6º, V)

Será realizado o levantamento de mercado para identificar as soluções disponíveis no mercado com capacidade para atender os requisitos técnicos estabelecidos pelas equipes da Superintendência de Tecnologia da Informação. Este levantamento envolverá:

- Análise de sites de fornecedores, comparativos de mercado, avaliações de usuários e artigos especializados.
- Realização de consulta pública para obter detalhes sobre as soluções disponíveis no mercado, funcionalidades, modelos de precificação e termos de serviço.
- Busca por informações em eventos da indústria e webinars sobre segurança e performance web.
- Busca por opiniões de especialistas em segurança da informação e infraestrutura de TI, a exemplo do Gartner.

O objetivo deste levantamento é obter a visão abrangente das opções disponíveis, entender seus pontos fortes e fracos, e identificar as soluções que melhor se adequam às necessidades da SEF/MG.

3.2. Estimativa do valor da contratação (art. 6º, VI)

A estimativa do valor da contratação será baseada em:

- Análise dos diferentes modelos de precificação oferecidos (por tráfego, por número de domínios, por funcionalidades, entre outras).
- Projeção do tráfego de dados da SEF/MG.
- Consideração do custo das funcionalidades específicas que serão necessárias.
- Avaliação do custo para atender à escala atual e futura da Secretaria.
- Comparação com os preços praticados no mercado por soluções similares.

3.3. Escolha da solução (consequência dos incisos V e VI do art. 6º)

A escolha das soluções será realizada com base em análise comparativa das opções levantadas no mercado, considerando os seguintes critérios:

- Avaliação de como cada solução atende aos requisitos técnicos e funcionais definidos no item 2.4 e detalhados no Termo de Referência
- Análise da relação entre o custo da solução e os benefícios que ela oferece em termos de segurança, performance e funcionalidades.
- Consideração da reputação do fornecedor no mercado, sua experiência com clientes similares e a qualidade do suporte técnico.
- Avaliação da complexidade da implementação e da integração da solução com a infraestrutura existente.
- Análise da capacidade da solução de escalar e se adaptar às futuras necessidades da SEF/MG.
- Avaliação da usabilidade e intuitividade da solução.

4. DETALHAMENTO DA SOLUÇÃO ESCOLHIDA

4.1. Descrição da solução como um todo (art. 6º, VII)

As soluções escolhidas devem oferecer um conjunto abrangente de serviços de segurança e performance. A arquitetura envolverá o roteamento do tráfego da internet destinado aos domínios e aplicações da SEF/MG por meio da rede global do fabricante.

- O WAF inspecionará o tráfego HTTP/HTTPS em busca de padrões maliciosos e tentativas de exploração de vulnerabilidades, aplicando regras de segurança personalizadas e protegendo contra as vulnerabilidades do OWASP Top 10.
- A rede global do fabricante atuará como uma barreira contra ataques DDoS volumétricos e de camada de aplicação, absorvendo e mitigando o tráfego malicioso antes que ele atinja a infraestrutura da secretaria.
- A CDN armazenará em cache cópias do conteúdo estático e dinâmico nos servidores distribuídos globalmente, reduzindo a latência e acelerando o carregamento das páginas para os usuários, independentemente da localização geográfica deles.
- O serviço de DNS do fabricante deve oferecer alta disponibilidade e segurança, além de otimizações de performance.
- O fabricante facilitará o gerenciamento e a renovação de certificados SSL/TLS, garantindo a criptografia do tráfego entre os usuários e os servidores do órgão.
- O SSE é uma arquitetura de segurança convergente e nativa da nuvem que move os controles de segurança para mais perto do usuário, onde quer que ele esteja.
- As soluções deverão oferecer console de administração intuitiva para configurar e monitorar as funcionalidades de segurança e performance, além de gerar relatórios detalhados.

4.2. Justificativas para o parcelamento ou não da contratação

A possibilidade de divisão ou não dos componentes de uma solução em itens para serem licitados em separado está relacionada com o grau de interdependência técnica entre os seus componentes, o que não é possível no presente caso.

Sobre o tema, a doutrina (Marçal Justen Filho, Comentários à Lei de licitações e Contratos Administrativos, 11ª ed., Dialética, 2005, p. 207) entende que a obrigatoriedade contida no § 1º do art. 23 deve respeitar limites de ordem técnica e econômica:

"Não se admite o fracionamento quando tecnicamente isso não for viável ou, mesmo, recomendável. O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. Não é possível desnaturar um certo objeto, fragmentando-o em contratações diversas e que importam o risco de impossibilidade de execução satisfatória."

Na mesma obra citada, p. 217, Marçal Justen Filho ensina que, em determinados tipos de contrato na área

de Tecnologia da Informação, a adoção de “Soluções Integradas” não pressupõe violação ao dever de parcelamento, in verbis:

"O objeto do contrato corporativo envolve o que passou a denominar-se de solução integrada. Trata-se de uma cumulação de prestações, envolvendo fornecimento e adequação de programas, sua manutenção, suporte técnico e chegando até à hipótese de treinamento de empregados. [...]. Essa alternativa desenvolveu-se a partir da constatação comum, reiteradamente experimentada, da inviabilidade da obtenção de resultados satisfatórios por meio de fornecedores autônomos diversos.”

Sob o ponto de vista econômico a contratação única evita ônus administrativos e burocráticos consequentes à contratação concomitante de mais de uma empresa fornecedora, e gera economia de escala, tempo, ganhos de eficiência e maior compromisso da empresa a ser contratada, sem restrição a competitividade.

Sob o ponto de vista técnico, adquirir uma plataforma unificada, fornecida por fabricante único, traz consigo benefícios significativos. A compatibilidade entre os componentes é intrínseca, eliminando problemas de integração e garantindo um funcionamento mais harmonioso e eficiente do sistema como um todo. Testes e validações são realizados de forma integrada, o que reduz a probabilidade de falhas e otimiza o desempenho. Além disso, a padronização de interfaces e protocolos simplifica a manutenção, o diagnóstico de problemas e futuras atualizações, representando uma arquitetura mais coesa e robusta.

A aquisição de forma integral das plataformas Web Application and API Protection e Security Service Edge de fabricante único atende os requisitos técnicos objetivados pela Superintendência de Tecnologia da Informação, razão pela qual as funcionalidades que fazem parte de cada uma delas deve ser de fabricante único.

4.3. Contratações correlatas e/ou interdependentes (art. 6º, XI)

Para a presente contratação não existem outras contratações correlatas ou interdependentes.

4.4. Resultados pretendidos (art. 6º, IX)

Com a contratação e implementação das referidas soluções, a SEF/MG espera alcançar os seguintes resultados:

- Redução significativa da exposição a ataques cibernéticos, protegendo os serviços online contra ameaças como DDoS, explorações de vulnerabilidades e bots maliciosos.
- Otimização do tempo de carregamento das páginas e redução da latência no acesso aos serviços online, proporcionando melhor experiência ao usuário.
- Garantia da continuidade dos serviços online, mesmo em caso de ataques ou picos de tráfego.
- Obtenção de informações detalhadas sobre o tráfego de internet e as ameaças, permitindo resposta mais rápida e eficaz a incidentes de segurança.
- Capacidade de lidar com o crescimento do tráfego e a adição de novos serviços online sem comprometer a segurança e a performance.
- Fortalecimento das medidas de segurança para atender a requisitos regulatórios e padrões da indústria.
- Potencial redução de custos relacionados a incidentes de segurança, perda de produtividade devido à indisponibilidade dos serviços e necessidade de investimentos em infraestrutura de segurança pontual.
- Segurança inteligente, adaptativa e distribuída, alinhada às necessidades da Secretaria.

Ao alcançar esses objetivos, a SEF/MG estará melhor posicionada para enfrentar os desafios cibernéticos contemporâneos, fortalecendo sua postura de segurança e preservando a integridade das operações e dos dados críticos.

4.5. Providências a serem adotadas (art. 6º, X)

Tendo em vista que o objeto da contratação pretendida é viabilizar a utilização das soluções de Web Application and API Protection e Security Service Edge com a infraestrutura da

CONTRATANTE, eventuais ajustes no ambiente serão realizados oportunamente, conforme orientação dos fornecedores do serviço.

4.6. Possíveis impactos ambientais (art. 6º, XII)

Inexistem riscos ambientais decorrentes desta contratação.

5. JUSTIFICATIVA ACERCA DOS CRITÉRIOS DE SUSTENTABILIDADE

Dada a natureza do objeto, considera-se que a presente aquisição atende aos requisitos de sustentabilidade nos termos do Relatório de Sustentabilidade SEF/MG Doc. (SEI nº 91207279).

6. POSICIONAMENTO CONCLUSIVO (ART. 6º, XIII)

Pelo presente estudo, em harmonia com o disposto nos normativos aplicáveis, bem como com as melhores práticas de mercado recomendadas, considerando a análise das alternativas de atendimento às necessidades elencadas pelas áreas requisitantes e quanto aos demais aspectos legais, conclui-se pela viabilidade da contratação, uma vez considerados os seus potenciais benefícios em termos de eficácia, eficiência, efetividade e economicidade. Em complemento, os requisitos listados atendem adequadamente às demandas formuladas, os custos previstos são compatíveis e os riscos identificados são administráveis, pelo que recomendamos o prosseguimento da contratação.

ASSINATURAS:

- Equipe de Planejamento da Contratação e Autoridade Competente nos termos do art. 5º da Resolução SEPLAG nº 115/2021.

Documento assinado eletronicamente por **Daniel de Oliveira Rezende**, **Servidor Público**, em 23/07/2025, às 17:29, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Rogério Zupo Braga**, **Superintendente**, em 28/07/2025, às 10:50, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **112396591** e o código CRC **0EBC24B5**.