Anexo nº I/SEF/STI-GOVERNANÇA-DSI/2025

PROCESSO Nº 1190.01.0006603/2025-21

Item	Requisitos (para demonstração e/ou apresentação de documentação oficial)	Atende? (sim / sim parcialmente / não)	Observações
1	**Web Application and API Protection**		
1.1	**Características Gerais da Solução**		
1.1.1	A solução deve oferecer os seguintes serviços em uma única plataforma integrada do fabricante: • Distribuição de conteúdo de rede - CDN; • Firewall de aplicação web - WAF • Segurança API • Mitigação Contra Ataques Distribuídos de Negação de Serviço – DDoS; • Gerenciamento de Robôs; • Validação de Usuários		
1.1.2	Os serviços devem ser prestados por meio de uma plataforma web unificada do fabricante e não intrusiva, ou seja, sem a necessidade de instalação de equipamentos no ambiente da Secretaria de Estado de Fazenda de Minas Gerais (SEF/MG);		
1.1.3	A solução deve prover serviço de bloqueio de acessos indevidos, visando evitar que tentativas de ataque sejam contabilizados, para não consumir a franquia contratada pela SEF/MG;		
1.1.4	A CDN deve fornecer o serviço de controle de camada IP para bloqueio ou liberação de endereços IP. Tais listas devem ser propagadas por toda a infraestrutura da Rede de Distribuição de Conteúdo;		

1.1.5	A CDN deve possuir capacidade de ocultar os websites e aplicações, restringindo o acesso dos usuários diretamente na origem, fornecendo uma camada adicional de proteção, através de uma lista definida de endereços IPs que têm permissão para se comunicar com a origem da aplicação;		
1.1.6	A CDN deve suportar a criação de listas de bloqueio ou liberação de sub-redes;		
1.1,7	Deve ser provido de serviço DNS autoritativo em nuvem, visando acelerar a resolução de nomes e proteger contra os ataques aos serviços de DNS da SEF/MG;		
1.1.8	O serviço DNS deve ser 100% compatível com DNSSEC, conforme regras do Registro.br para domínios com o sufixo GOV.BR.		
1.1.9	A solução deve possuir suporte a zona de pesquisa direta e zona de pesquisa inversa.		
1.1.10	Deve ser provido serviço de detecção, identificação e gestão de robôs (botnets), de forma a proteger os websites e as aplicações da SEFAZ-MG;		
1.1.11	O fabricante deve possuir ao menos uma das seguintes certificações de compliance SOC 2 Tipo 2, ISO 27001 ou ISO 27018.		
1.2	**Rede Dinâmica de Distribuição e Aceleração De Conteúdo - CDN**		
1.2.1	A CDN deve ser descentralizada e sem ponto único de falha, com servidores distribuídos para entrega de conteúdo estático ou dinâmico de forma criptografada (TLS/SSL) em todos os pontos da rede;		
1.2.2	Cada data center deve possuir servidores de distribuição de conteúdo e segurança em número suficiente para manter o SLA de 99,999% de disponibilidade;		
1.2.3	A solução deve possuir algoritmo de roteamento dinâmico para redirecionamento do tráfego, sem prejuízo ao desempenho dos serviços, no caso de indisponibilidade de qualquer datacenter;		

1.2.4	A solução deve possuir ambiente de testes de configurações, em que seja possível aplicar todas as funcionalidades de distribuição de conteúdo e segurança, a fim de validar todas as configurações do website ou aplicação antes de publicar em produção.		
1.2.5	A solução deve fazer uso de algoritmos para determinar qual servidor da rede dinâmica possui melhores condições de entrega, utilizando métodos para o redirecionamento do usuário, desde servidores de aplicações, até o redirecionamento no nível de Servidor de Domínio de Nomes (Domain Name Servers, DNS);		
1.2.6	A solução deve prover disponibilidade dos sites e tempo de carregamento das páginas inferior ao de carregamento sem o uso da CDN, independentemente da quantidade de usuários e dados acessados simultaneamente;		
1.2.7	A solução deve permitir realizar a expiração de conteúdo wildcard, em toda a rede		
1.2.8	A solução deve permitir realizar a expiração de conteúdo (purge) por URL, em um prazo máximo de 5 minutos;		
1.2.9	A solução deve possuir caminhos redundantes de acesso e distribuição de conteúdo, a fim de garantir o acesso a seus serviços, bem como ao serviço de origem;		
1.2.10	A solução deve acelerar e distribuir indistintamente quaisquer aplicações baseadas em Protocolo de Transferência de Hipertexto (Hypertext Transfer Protocol, HTTP e HTTPS), balanceando entre seus POPs, a carga das páginas de modo a garantir melhor performance;		
1.2.11	Para a aceleração e distribuição de aplicações HTTPS, a contratada deve realizar, sem custos adicionais para a SEF/MG, a emissão dos certificados digitais necessários para o funcionamento de endereços em SSL;		

1.2.12	A solução deve identificar falhas, caso haja indisponibilidade em um dos links usados no datacenter de origem, para contínua transmissão e entrega do conteúdo;		
1.2.13	A solução deve tratar de maneira individualizada as requisições maliciosas direcionadas aos sites WEB da origem e bloqueá-la;		
1.2.14	Para evitar falso positivos, a CDN deve implementar análise e inspeção de corpo de requisições, não limitando-se apenas a assinaturas;		
1.2.15	A solução deve responder a diferentes métodos HTTP, considerando, pelo menos: GET, HEAD, POST, PUT, PATCH, DELETE e OPTIONS;		
1.2.16	A solução deve fornecer o serviço de geolocalização a nível de país, que permitirá o gerenciamento de listas de permissão e negação de acessos;		
1.2.17	O painel de monitoramento deve disponibilizar informações como: país, endereço IP, descrição da ameaça/regra que está sendo processada, método HTTP utilizado, data e hora da ocorrência da CDN. Deve conter, informações acerca das atividades maliciosas processadas, apresentando: • Quais sites WEB estão sendo atacados; • O que está sendo explorado no ataque;		
1.2.18	O painel de monitoramento deve apresentar e contabilizar, através de gráficos, todas as requisições de conteúdo realizadas pelo usuário final para todo e qualquer código de status HTTP/HTTPS, gerando relatórios por período, permitindo a identificação dos picos de acesso a CDN;		
1.2.19	O painel de monitoramento deve apresentar e contabilizar, através de gráficos e API, o volume de dados trafegado e requisições entre a CDN e o usuário final para todo e qualquer código de status HTTP/HTTPS da CDN;		

1.2.20	O painel de monitoramento deve apresentar e contabilizar, através de gráficos e API, o volume de dados trafegado e requisições buscadas a partir da origem ou entregues a partir dos servidores de borda da plataforma da CDN;		
1.2.21	O painel de monitoramento deve disponibilizar os Logs das informações dos servidores para download, em intervalo não superior a 1 (uma) hora da CDN;		
1.2.22	O painel de monitoramento deve permitir o monitoramento real de navegação dos visitantes, conforme abaixo: • Monitoramento de usuários por meio de injeção de JavaScript no HTML para monitorar dados de desempenho e informações do cliente; • Monitoramento do desempenho de navegação dos visitantes dos sites protegidos pela plataforma coletando beacons por meio de injeção automática de código para as principais plataformas móveis do mercado (Android e iOS) e principais navegadores de internet (Google Chrome, Firefox e MS Edge); • Permitir o acompanhamento em tempo real dos dados de desempenho coletados pelos beacons, fornecendo visualização de, no mínimo, as seguintes dimensões: navegador, dispositivo, Sistema Operacional e localidade geográfica; • A CDN deve disponibilizar via API a consulta e a alteração das configurações de cache e regras de segurança com reflexo em todos os servidores de borda da plataforma.		
1.3	**Segurança de Firewall de Aplicação Web (WAF)**		

1.3.1	A solução ofertada deve disponibilizar em todos os Pontos de Presença o serviço de WAF – firewall de aplicação - para impedir atividades maliciosas, incluindo pelo menos as seguintes funcionalidades, além de outros tipos de ataques comuns e vulnerabilidades conhecidas a serem bloqueadas: • Bloqueio por rede e IP; • Geolocalização; • Secure token; • Cross site scripting (XSS); • Remote file inclusion (RFI); • Directory transversal; • SQL injection.		
1.3.2	A solução deve possuir proteção contra as vulnerabilidades WEB listadas no OWASP TOP 10, descritas abaixo: • Broken Access Control; • Cryptographic Failures; • Injection; • Insecure Design; • Security Misconfiguration; • Vulnerable and Outdated Components; • Identification and Authentication Failures; • Software and Data Integrity Failures; • Security Logging and Monitoring Failures; • Server-Side Request Forgery - SSRF;		
1.3.3	A solução deve possuir proteção contra exploração de vulnerabilidade (exploit) por meio de inspeções de regras WAF.		
1.4	**Mitigação Contra Ataques Distribuídos de Negação de Serviço – DDoS**		

1.4.1	A solução deve prover serviço de defesa, visando mitigar os efeitos de ataques de Distributed Denial-Of-Service (DDoS), sobre o conteúdo distribuído através dos servidores de borda, evitando que estes ataques alcancem a origem dos dados;		
1.4.2	A solução deve mitigar ataques de forma transparente, absorvendo e bloqueando ataques de TCP/IP SYN flood nos seus endereços IP mantendo a disponibilidade do serviço e entrega das aplicações;		
1.4.3	A solução deve fornecer o serviço de detecção e mitigação de ameaças para tráfego HTTP e HTTPS. O serviço deve continuar escalável instantaneamente e manter alta performance;		
1.4.4	A solução deve absorver e tratar as ameaças WEB na origem do ataque, absorvendo o tráfego malicioso e criando proteção de perímetro dentro da Internet.		
1.5	**Proteção de API**		
1.5.1	A solução deve ser capaz de proteger as APIs implantadas para aplicações com base em pelo menos: • SOAP; • XML; • API JSON; • API RESTful.		
1.5.2	A solução deve ser capaz de inspecionar o tráfego criptografado com TLS 1.2, 1.3 e rastrear o comportamento de uso, para identificar o uso suspeito;		
1.5.3	A solução deve ser capaz de fazer descoberta automaticamente e continuamente dos pontos de exposição de API públicos e seus esquemas;		
1.5.4	A solução deve ser capaz de customizar regras para as APIs gerenciadas como uma medida de segurança adicional;		
1.5.5	A solução deve ter a capacidade de proteger as APIs associadas aos sites protegidos;		

1.5.6	A solução deve permitir fornecer segurança API com base em seu arquivo de especificação, gerando automaticamente um modelo de segurança positivo que protege contra os riscos de segurança associados;		
1.5.7	A solução deve detectar e bloquear qualquer acesso a métodos não contidos na API como uma violação;		
1.5.8	A solução deve possuir proteção DDoS por meio de controles de taxa (rate limit).		
1.6	**Gerenciamento de Robôs**		
1.6.1	A solução deve detectar o acesso de robôs nos sites do SEF/MG;		
1.6.2	A solução deve possuir uma lista dinâmica de robôs já categorizados e conhecidos (Bots Bons). A lista deve ser atualizada automaticamente para incluir novos bots ou remover bots que desaparecem;		
1.6.3	A solução deve ser capaz de detectar imitadores de bots conhecidos, diferenciando através do cabeçalho do User-Agent a botnet real e seu imitador;		
1.6.4	A solução deve ser capaz de detectar bots criados por meio de Estruturas de Desenvolvimentos Comuns, Bibliotecas HTTP, Bibliotecas de Serviços Web, Rastreadores, Ferramentas de Automação e Web Crawlers;		
1.6.5	Deve ser capaz de detectar o acesso de robôs avaliando os aspectos e anomalias da requisição como assinatura de cabeçalhos incorretas, cabeçalhos fora de ordem e incompatibilidade de versão do navegador;		
1.6.6	A solução deve ser capaz de criar categoria de bots personalizada, permitindo que bots específicos sejam definidos como bots amigáveis;		

1.6.7	A solução deve ser capaz de aplicar ações de segurança para os robôs, permitindo, no mínimo, as seguintes opções: • Monitorar o acesso, para avaliação do tráfego de robôs; • Permitir o acesso; • Bloquear o acesso e retornar código de erro HTTP 403 (acesso negado); • Bloquear o acesso e retornar com mensagem customizada.		
1.7	**Validação de Usuários**		
1.7.1	A solução deve possuir solução de validação de usuários, por meio de análise de comportamento e métricas coletadas pelo navegador;		
1.7.2	A solução deve suportar a autenticação automática de usuários sem a necessidade de desafios visuais, utilizando análises de comportamento e sinais do navegador para validar a interação humana.		
1.7.3	A solução deve permitir os seguintes modos de desafios: com interação do usuário, em segundo plano sem interação do usuário e operação sem indicação visual ao usuário;		
1.7.4	Deve ser compatível com os principais navegadores e dispositivos móveis;		
1.7.5	A solução deve fornecer métricas detalhadas e relatórios sobre o desempenho dos desafios, incluindo número de desafios emitidos e taxas de resolução.		
1.7.6	A solução deve suportar integração com aplicações web utilizando HTML e JavaScript, permitindo renderização implícita (automática) ou explícita (controlada via código).		
1.7.7	A solução deve permitir a configuração e gestão de widgets através de API, incluindo operações de criação, atualização e exclusão de widgets.		

1.7.8	A solução deve suportar a emissão de cookies de pré-liberação (pre-clearance) para simplificar a experiência do usuário em aplicações de página única (SPAs), permitindo que usuários confiáveis evitem desafios adicionais.		
1.7.9	A solução deve garantir que tokens gerados sejam únicos e válidos por um curto período, prevenindo reutilização indevida e garantindo a integridade das validações.		
1.7.10	A solução deve permitir a rotação de chaves secretas utilizadas na comunicação entre o widget e o servidor, assegurando a segurança contínua da solução.		
2	**Proteção DNS**		
2.1	A contratada deve prover solução em nuvem para os serviços de DNS autoritativo para 4 (quatro) Zonas SEF/MG;		
2.2	Os serviços fornecidos deverão ser do tipo DNSSEC (Domain Name System Security Extensions);		
2.3	A solução deve ter ao menos um ponto de presença para resolução de DNS no Brasil;		
2.4	O serviço deve prover disponibilidade de DNS 24x7x365, com nível de serviço de 99,999%;		
2.5	A Plataforma deve prover mecanismos para aceleração de resolução de nomes DNS;		
2.6	A solução deve implementar o serviço como DNS primário ou secundário, substituindo ou aumentando a infraestrutura DNS da SEF/MG;		
2.7	A plataforma de DNS em nuvem deve prover: • Aceleração de resolução DNS; • Proteção contra ataques DNS; • Mecanismos que possibilitem a alta disponibilidade do serviço DNS; • Mecanismos para manutenção da configuração de DNS para os sítios a serem protegidos.		

2.8	A contratada deve prover interface de gerenciamento dos serviços de DNS por meio de portal em nuvem e por meio de interfaces de programação de aplicação (APIs), permitindo integrações com ferramentas da SEF/MG.		

Documento assinado eletronicamente por **Daniel de Oliveira Rezende**, **Servidor Público**, em 23/07/2025, às 17:30, 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 10:57, 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 **113522336** e o código CRC **BFE2656B**.