GOVERNO DO ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
Divisão de Segurança da Informação

Belo Horizonte, 28 de abril de 2025.

Termo de Referência de Prestação de Serviços SEF/STI-GOVERNANÇA-DSI Nº 1/2025

TERMO DE REFERÊNCIA DE PRESTAÇÃO DE SERVIÇOS

MINUTA PADRONIZADA DE TERMO DE REFERÊNCIA PARA CONTRATAÇÃO DE SERVIÇOS PELOS CRITÉRIOS DE JULGAMENTO MENOR PREÇO OU MAIOR DESCONTO (PREGÃO ELETRÔNICO)

ANEXO I – TERMO DE REFERÊNCIA DE PRESTAÇÃO DE SERVIÇOS

DATA	ÓRGÃO/ENTIDADE SOLICITANTE	NÚMERO DA UNIDADE DE COMPRA
22/07/2025	Secretaria de Estado de Fazenda	1191001

RESPONSÁVEL PELA SOLICITAÇÃO	SUPERINTENDÊNCIA OU DIRETORIA OU UNIDADE ADMINISTRATIVA
Nome: Equipe de Planejamento da Contratação E-mail: stidgvdce@fazenda.mg.gov.br	Superintendência de Tecnologia da Informação / Diretoria de Governança - STI/DGV

SUMÁRIO

1. OBJETO E CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. O presente Termo de Referência tem por objeto a 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), além de 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, sem dedicação exclusiva de mão de obra, nos termos da tabela abaixo e conforme condições e exigências estabelecidas neste documento.

LOTE	ITEM	CÓD. DO ITEM NO CATMAS	DESCRIÇÃO DO ITEM CATMAS	UNIDADE DE MEDIDA	QUANTIDADE
1	1		Solução WAAP, com WAF/Anti-DDoS e certificados SSL e TLS, com franquia de 5 TB de tráfego limpo ou throughput mensal equivalente	Unidade	1
	2		Franquia adicional de tráfego limpo a ser consumido e cobrado sob demanda durante a vigência contratual	Unidade	100 TB ou Throughput equivalente
	3		Proteção de DNS	Unidade	1
	4	134872	Serviços de instalação, configuração, teste em produção e ajuste	Unidade	1
	5	107590	Treinamento de solução de segurança	Unidade	6
2	1		Solução de SSE (Security Service Edge)	Unidade	3500
	2	134872	Serviços de instalação, configuração, teste em produção e ajuste	Unidade	1
	3	107590	Treinamento de solução de segurança	Unidade	6

1.2. **Caracterização do Objeto**

1.2.1. O objeto desta contratação é caracterizado como comum, pois apresenta padrões de desempenho e qualidade objetivamente definidos por meio de especificações usuais de mercado.

1.3. **Lotes Exclusivos para Microempresas e Empresas de Pequeno Porte**

1.3.1. A participação na presente licitação é aberta a todos (sem exclusividade ou reserva de lotes para Microempresas, Empresas de Pequeno Porte e equiparados aos benefícios do Decreto nº 47.437, de 2018 e Lei Complementar nº 123, de 2006).

1.4. **Da Contratação**

1.4.1. O prazo de vigência da contratação é de 1 (um) ano, podendo os itens 1 dos Lotes 1 e 2 serem prorrogados por até 10 (dez) anos, contado do primeiro dia útil subsequente à divulgação no Portal Nacional de Contratações Públicas (PNCP), na forma dos arts. 106 e 107 da Lei Federal nº 14.133, de 2021.

1.4.2. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

1.5. **Do Reajuste**

1.5.1. Durante o prazo de vigência, os preços contratados poderão ser reajustados monetariamente com base no ICTI - Índice de Custo da Tecnologia da Informação, mantido pelo Ipea - Instituto de Pesquisa Econômica Aplicada, observado o interregno mínimo de 12 (doze) meses, contados do orçamento estimado, em 24/09/2024 (97235281), nos termos do art. 92, §§ 3º e 4º, da Lei nº 14.133/2021.

1.6. **Descrição da Solução**

1.6.1. **Lote 1 - Item 1 - Solução WAAP, com WAF/Anti-DDoS e certificados SSL e TLS, com franquia de 5 TB de tráfego limpo ou throughput mensal equivalente**

1.6.1.1. **Características Gerais da Solução**

1.6.1.1.1. A solução deve oferecer os seguintes serviços:

1.6.1.1.1.1. Distribuição de conteúdo de rede - CDN;

1.6.1.1.1.2. Firewall de aplicação web – WAF;

1.6.1.1.1.3. Segurança API;

1.6.1.1.1.4. Mitigação Contra Ataques Distribuídos de Negação de Serviço – DDoS;

1.6.1.1.1.5. Gerenciamento de Robôs;

1.6.1.1.1.6. Validação de Usuários

1.6.1.1.2. Os serviços devem ser prestados por meio de plataforma web unificada 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);

1.6.1.1.3. A rede CDN e o WAF devem estar disponíveis mediante alteração do DNS da SEF/MG;

1.6.1.1.4. Os serviços contratados serão contabilizados por volume de tráfego ou throughput mensal entregue pela plataforma;

1.6.1.1.5. Será contratada franquia base de volume de tráfego mensal entregue pela plataforma de 5 Terabytes (TB), ou um throughput mensal que corresponda a este volume;

1.6.1.1.6. O fabricante que decidir ofertar o serviço em throughput deve detalhar a métrica utilizada para garantir a correspondência com o volume entregue de 5 TB mensais;

1.6.1.1.7. Deve ser considerado para apuração do tráfego, somente o conteúdo legítimo entregue à Secretaria pelos servidores de borda. Não será aceita cobrança por ataque ou por tráfego entre os servidores da rede de distribuição de conteúdo;

1.6.1.1.8. Será contratada franquia adicional de volume de tráfego excedente, a ser consumido após o esgotamento do tráfego mensal contratado;

1.6.1.1.9. 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;

1.6.1.1.10. 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;

1.6.1.1.11. 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, por meio de uma lista definida de endereços IPs que têm permissão para se comunicar com a origem da aplicação;

1.6.1.1.12. A CDN deve suportar a criação de listas de bloqueio ou liberação de sub-redes;

1.6.1.1.13. Deve ser provido serviço DNS autoritativo em nuvem, visando acelerar a resolução de nomes e proteger contra os ataques aos serviços de DNS da SEF/MG;

1.6.1.1.14. O serviço DNS deve ser 100% compatível com DNSSEC, conforme regras do Registro.br para domínios com o sufixo GOV.BR.

1.6.1.1.15. A solução deve possuir suporte à zona de pesquisa direta e à zona de pesquisa inversa.

1.6.1.1.16. Deve ser provido serviço de detecção, identificação e gestão de robôs (botnets), de forma a proteger os websites e as aplicações da SEF/MG;

1.6.1.1.17. O fabricante deve possuir ao menos uma das seguintes certificações de compliance SOC 2 Tipo 2, ISO 27001 ou ISO 27018.

1.6.1.1.18. Para garantir segurança e agilidade na gestão da solução, é recomendável que todos os módulos de segurança (WAF, BOT, DNS, DoS, API) sejam gerenciados por meio de console única, de forma que todas as configurações e monitoramento possam ser feitos de forma centralizada.

1.6.1.2. **Rede Dinâmica de Distribuição e Aceleração De Conteúdo - CDN**

1.6.1.2.1. A solução deve ter ao menos um ponto de presença no Brasil;

1.6.1.2.2. 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;

1.6.1.2.3. Cada data center deve possuir servidores de distribuição de conteúdo e segurança em número suficiente para manter o SLA de 99,999% de disponibilidade;

1.6.1.2.4. 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;

1.6.1.2.5. 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.

1.6.1.2.5.1. Este ambiente deve possuir servidores em nuvem específicos e dedicados para realização dos testes das novas configurações;

1.6.1.2.5.2. A área de teste das funcionalidades especificadas neste artefato de Termo de Referência, deve possuir todas as funcionalidades do ambiente de produção;

1.6.1.2.5.3. O ambiente deve possuir endereços IPs ou hostnames específicos que devem ser usados nos testes, possibilitando que seja testada todas as funcionalidades dos websites ou aplicações protegidas, apenas realizando o direcionamento do navegador do cliente para este ambiente;

1.6.1.2.5.4. A solução deve ser possível aplicar a mesma configuração do ambiente de teste no ambiente de produção, diretamente na interface de gerência;

1.6.1.2.5.5. Com a solução em produção, deve disponibilizar simultaneamente o ambiente de teste para criação e validação de novas versões de configuração, sem

que a versão em produção seja afetada;

1.6.1.2.6. 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);

1.6.1.2.7. A solução deve ser configurada para habilitar todos os seus servidores a reconhecer o site de origem, seus conteúdos estáticos (CSS, JS, documentos, imagem, vídeo, áudio, dentre outros) e dinâmicos, tanto no Brasil quanto no exterior;

1.6.1.2.8. A contratada deve prover aceleração e proteção para no mínimo 300 (trezentos) FQDNs pertencentes à SEF/MG, registradas sob o domínio https://www.fazenda.mg.gov.br/.

1.6.1.2.9. 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;

1.6.1.2.10. A solução deve propagar as mudanças nas listas de liberação e bloqueio em até 10 minutos, permitindo assim a resposta a incidentes de segurança na infraestrutura da SEF/MG;

1.6.1.2.11. A solução deve permitir realizar a expiração de conteúdo wildcard, em toda a rede

1.6.1.2.12. A solução deve permitir realizar a expiração de conteúdo (purge) por URL, em um prazo máximo de 5 minutos;

1.6.1.2.13. 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;

1.6.1.2.14. 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;

1.6.1.2.15. Para a aceleração e distribuição de aplicações HTTPS, a contratada deve realizar, sem custos adicionais, a emissão dos certificados digitais necessários para o funcionamento de endereços SSL;

1.6.1.2.16. Após a configuração dos certificados, deverão ser realizados testes utilizando a ferramenta Qualys SSL Labs (https://www.ssllabs.com/ssltest/) ou outra similar, na qual deve ser obtida a qualificação “A” para todas as URLs;

1.6.1.2.17. Os Certificados Digitais A1 SSL/TLS para Servidor Web deverão ter as seguintes especificações:

1.6.1.2.17.1. Os certificados emitidos deverão ser do tipo A1 SSL/TLS para Servidor Web, podendo ser individualizados para cada URL implantada ou do tipo wildcard em que o certificado permite que seja adicionada segurança SSL a ilimitados sites, desde que façam parte de subdomínios de um mesmo domínio;

1.6.1.2.17.2. Todos os certificados emitidos deverão possuir o certificado raiz da autoridade certificadora dentre as que já vêm previamente instaladas e configuradas nos principais navegadores e dispositivos do mercado suportando, no mínimo: Mozilla Firefox, Google Chrome, Microsoft Edge, Safari, iPhone, Android e Windows Phone;

1.6.1.2.17.3. A CONTRATADA deve manter o certificado válido durante todo o período do contrato;

1.6.1.2.17.4. O procedimento para validação dos certificados deve ser on-line, telefônico ou via validação de DNS;

1.6.1.2.17.5. A fornecedora deve possuir a capacidade de configuração das cifras

e da versão de TLS utilizada pela SEF/MG;

1.6.1.2.17.6. A solução deve possuir validação da organização emissora do certificado digital, incluindo os dados da SEF/MG, conforme o caso, no certificado digital;

1.6.1.2.18. A solução deve identificar falhas, caso haja indisponibilidade em um dos links usados no datacenter de origem, para contínua transmissão e entrega do conteúdo;

1.6.1.2.19. A solução deve suportar a configuração de uma origem principal e outra backup (standby), que só será utilizada em caso de falha da primeira;

1.6.1.2.20. A solução deve ser sensível à existência de letras maiúsculas e minúsculas para armazenamento de objetos em cache;

1.6.1.2.21. A solução deve permitir a seleção de argumentos de query strings e cookies para armazenamento de objetos em cache, fazendo com que o objeto armazenado em cache seja o mesmo para solicitações com características afins;

1.6.1.2.22. A solução deve possuir os seguintes recursos para a gestão de cache:

1.6.1.2.22.1. Suporte a não armazenagem (no store);

1.6.1.2.22.2. Opção para ignorar cache (bypass cache), nesse caso o conteúdo do cache não será armazenado pela CDN.

1.6.1.2.23. A solução deve tratar de maneira individualizada as requisições maliciosas direcionadas aos sites WEB da origem e bloqueá-la;

1.6.1.2.24. A solução deve permitir a criação de políticas de cache que permitam não fazer cache da requisição (bypass) assim como encaminhar os cookies tal como enviados pelos usuários para os servidores de origem;

1.6.1.2.25. Para evitar falso positivos, a CDN deve implementar análise e inspeção de corpo de requisições, não limitando-se apenas a assinaturas;

1.6.1.2.26. A solução deve responder a diferentes métodos HTTP, considerando, pelo menos: GET, HEAD, POST, PUT, PATCH, DELETE e OPTIONS;

1.6.1.2.27. A solução deve restringir para determinado site, métodos HTTP específicos, bloqueando outros métodos que não forem habilitados;

1.6.1.2.28. A solução deve modificar, adicionar ou remover informações do cabeçalho HTTP durante a comunicação com os datacenters de origem;

1.6.1.2.29. A solução deve permitir a implementação de redirecionamento HTTP otimizando a comunicação com o datacenter de origem;

1.6.1.2.30. A solução deve fornecer o serviço de geolocalização a nível de país, que permitirá o gerenciamento de listas de permissão e negação de acessos;

1.6.1.2.31. A solução deve realizar a entrega de qualquer formato e tipo de conteúdo nos protocolos HTTP 1.1 e 2;

1.6.1.2.32. A solução deve prover aceleração através da compressão de dados desde que suportado pelo navegador ou dispositivo utilizado pelo usuário;

1.6.1.2.33. A solução deve detectar as características dos dispositivos por meio das informações de navegador de Internet;

1.6.1.2.34. A solução deve permitir a obtenção de objetos checados a partir de outros servidores da rede, evitando assim conexão com o datacenter de origem;

1.6.1.2.35. A solução deve verificar que a requisição está sendo feita por um site autorizado a ter acesso ao conteúdo armazenado;

1.6.1.2.36. A solução deve possuir recurso de defesa ativa imediata;

1.6.1.2.37. A solução deve prover a infraestrutura necessária para a adequada

prestação dos serviços indicados anteriormente, de forma escalável, automaticamente e em tempo real, independentemente da quantidade de acessos simultâneos;

1.6.1.2.38. Por meio do painel de monitoramento deve ser possível subdividir e permitir a consulta de dados referente a tráfego, requisições HTTP e HTTPS, hits, exclusivamente para cada site WEB configurado, permitindo a geração de relatórios específicos para cada site presente na CDN para, no mínimo, 30 dias de histórico;

1.6.1.2.39. O painel de monitoramento deve possuir opções para geração de filtros, possibilitando a criação de relatórios customizados por site e data;

1.6.1.2.40. O painel de monitoramento deve permitir acompanhar o quantitativo de requisições realizadas para cada site WEB na CDN;

1.6.1.2.41. 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:

1.6.1.2.41.1. Quais sites WEB estão sendo atacados;

1.6.1.2.41.2. O que está sendo explorado no ataque;

1.6.1.2.42. O painel de monitoramento deve apresentar as informações e permitir a consulta da CDN;

1.6.1.2.43. O painel de monitoramento deve apresentar e contabilizar, por meio 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 à CDN;

1.6.1.2.44. O painel de monitoramento deve apresentar e contabilizar, por meio 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;

1.6.1.2.45. O painel de monitoramento deve apresentar e contabilizar, por meio 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;

1.6.1.2.46. O painel de monitoramento deve disponibilizar os Logs das informações dos servidores para download;

1.6.1.2.47. O painel de monitoramento deve permitir o monitoramento real de navegação dos visitantes, conforme abaixo:

1.6.1.2.47.1. Monitoramento de usuários para monitorar dados de desempenho e informações do cliente;

1.6.1.2.47.2. Monitoramento do desempenho de navegação dos visitantes dos sites protegidos pela plataforma coletando beacons para as principais plataformas móveis do mercado (Android e iOS) e principais navegadores de internet (Google Chrome, Firefox e MS Edge);

1.6.1.2.47.3. 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;

1.6.1.2.47.4. 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.

1.6.1.3. **Segurança de Firewall de Aplicação Web (WAF)**

1.6.1.3.1. 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:

1.6.1.3.1.1. Bloqueio por rede e IP;

1.6.1.3.1.2. Geolocalização;

1.6.1.3.1.3. Secure token;

1.6.1.3.1.4. Cross site scripting (XSS);

1.6.1.3.1.5. Remote file inclusion (RFI);

1.6.1.3.1.6. Directory transversal;

1.6.1.3.1.7. SQL injection.

1.6.1.3.2. A solução deve possuir proteção contra as vulnerabilidades WEB listadas no OWASP TOP 10, descritas abaixo:

1.6.1.3.2.1. Broken Access Control;

1.6.1.3.2.2. Cryptographic Failures;

1.6.1.3.2.3. Injection;

1.6.1.3.2.4. Insecure Design;

1.6.1.3.2.5. Security Misconfiguration;

1.6.1.3.2.6. Vulnerable and Outdated Components;

1.6.1.3.2.7. Identification and Authentication Failures;

1.6.1.3.2.8. Software and Data Integrity Failures;

1.6.1.3.2.9. Security Logging and Monitoring Failures;

1.6.1.3.2.10. Server-Side Request Forgery - SSRF;

1.6.1.3.3. A solução deve possuir proteção contra exploração de vulnerabilidade (exploit) por meio de inspeções de regras WAF.

1.6.1.4. **Mitigação Contra Ataques Distribuídos de Negação de Serviço – DDoS**

1.6.1.4.1. A solução deve prover serviço de defesa, visando mitigar os efeitos de ataques de Distributed Denial-Of-Service (DDoS), sobre o conteúdo distribuído por meio dos servidores de borda, evitando que estes ataques alcancem a origem dos dados;

1.6.1.4.2. 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;

1.6.1.4.3. 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;

1.6.1.4.4. 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.

1.6.1.5. **Proteção de API**

1.6.1.5.1. A solução deve ser capaz de proteger as APIs implantadas para aplicações com base em pelo menos:

1.6.1.5.1.1. SOAP;

1.6.1.5.1.2. XML;

1.6.1.5.1.3. API JSON;

1.6.1.5.1.4. API RESTful.

1.6.1.5.2. A solução deve ser capaz de inspecionar o tráfego criptografado com TLS 1.2, 1.3 e rastrear o comportamento, para identificar o uso suspeito;

1.6.1.5.3. A solução deve ser capaz de fazer descoberta automaticamente e continuamente dos pontos de exposição de API públicas e seus esquemas;

1.6.1.5.4. A solução deve ser capaz de customizar regras para as APIs gerenciadas como uma medida de segurança adicional;

1.6.1.5.5. A solução deve ter a capacidade de proteger as APIs associadas aos sites protegidos;

1.6.1.5.6. 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;

1.6.1.5.7. A solução deve detectar e bloquear qualquer acesso a métodos não contidos na API como uma violação;

1.6.1.5.8. A solução deve ser integrada a mecanismos de análise de eventos de segurança;

1.6.1.5.9. A solução deve possuir proteção DDoS por meio de controles de taxa (rate limit).

1.6.1.5.10. A solução deve ser capaz de autenticar e validar o tráfego de API com certificados mTLS, utilizando certificado e chave intermediária de terceiros para autenticação da API e enviando o certificado de cliente para o servidor de aplicação por meio de um ou mais cabeçalhos.

1.6.1.6. **Gerenciamento de Robôs**

1.6.1.6.1. A solução deve detectar o acesso de robôs nos sites da SEF/MG;

1.6.1.6.2. A solução deve possuir uma lista dinâmica de robôs já categorizados e conhecidos. A lista deve ser atualizada automaticamente para incluir novos bots ou remover bots que desaparecem;

1.6.1.6.3. A solução deve ser capaz de detectar imitadores de bots conhecidos, diferenciando por meio do cabeçalho do User-Agent a botnet real e seu imitador;

1.6.1.6.4. 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;

1.6.1.6.5. A solução 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;

1.6.1.6.6. A solução deve ser capaz de criar categoria de bots personalizada, permitindo que bots específicos sejam definidos como bots amigáveis;

1.6.1.6.7. A solução deve ser capaz de aplicar ações de segurança para os robôs, permitindo, no mínimo, as seguintes opções:

1.6.1.6.7.1. Monitorar o acesso para avaliação do tráfego de robôs;

1.6.1.6.7.2. Permitir o acesso;

1.6.1.6.7.3. Bloquear o acesso e retornar código de erro HTTP 403 (acesso negado);

1.6.1.6.7.4. Bloquear o acesso e retornar com mensagem customizada.

1.6.1.7. **Validação de Usuários**

1.6.1.7.1. A solução deve possuir solução de validação de usuários, por meio de análise de comportamento e métricas coletadas pelo navegador;

1.6.1.7.2. 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.

1.6.1.7.3. 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;

1.6.1.7.4. A solução deve permitir a personalização da aparência do widget, oferecendo tamanhos como normal, flexível e compacto, além de temas claro e escuro.

1.6.1.7.5. A solução deve ser compatível com os principais navegadores e dispositivos móveis;

1.6.1.7.6. A solução deve fornecer métricas detalhadas e relatórios sobre o desempenho dos desafios, incluindo número de desafios emitidos e taxas de resolução.

1.6.1.7.7. A solução deve suportar integração com aplicações web utilizando HTML e JavaScript, permitindo renderização implícita (automática) ou explícita (controlada via código).

1.6.1.7.8. A solução deve permitir a configuração e gestão de widgets através de API, incluindo operações de criação, atualização e exclusão de widgets.

1.6.1.7.9. 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.

1.6.1.7.10. A solução deve garantir que tokens gerados sejam únicos e válidos por um curto período, prevenindo reutilização indevida e garantindo a integridade das validações.

1.6.1.7.11. A solução deve permitir a rotação de chaves secretas utilizadas na comunicação entre o widget e o servidor, assegurando a segurança contínua da solução.

1.6.2. **Lote 1 - Item 2 - Franquia Adicional de Tráfego**

1.6.2.1. A rede deve prover a infraestrutura necessária para a adequada prestação dos serviços especificados, de forma escalável, automaticamente e em tempo real, independentemente da quantidade de acessos simultâneos;

1.6.2.2. O painel de monitoramento deve disponibilizar ferramenta que permita a mensuração e controle em tempo real da utilização de tráfego eventualmente transportado. A ferramenta deve permitir a emissão de relatórios gerenciais com quantitativos e consumos por períodos da CDN;

1.6.2.3. Será contratada uma franquia adicional de volume de tráfego excedente pelo período do contrato, a ser consumido após o esgotamento da liberalidade de acessos nativa da infraestrutura implantada;

1.6.2.4. A franquia adicional será de até 50 (cinquenta) Terabytes estimado pelo período de 12 (doze) meses ou um throughput mensal que corresponda a este volume;

1.6.2.4.1. O desembolso será feito de forma proporcional à quantidade de TB utilizados calculados em intervalos de 5 (cinco) Terabytes.

1.6.2.5. A empresa que decidir por ofertar o serviço em throughput deve detalhar a métrica utilizada para garantir a correspondência com o volume adicional de 50 (cinquenta) Terabytes pelos 12 (doze) meses de duração do contrato.

1.6.3. **Lote 1 - Item 3 - Proteção DNS**

1.6.3.1. A contratada deve prover solução em nuvem para os serviços de DNS autoritativo para 4 (quatro) Zonas SEF/MG;

1.6.3.2. Os serviços fornecidos deverão ser do tipo DNSSEC (Domain Name System Security Extensions);

1.6.3.3. A solução deve ter ao menos um ponto de presença para resolução de DNS no Brasil;

1.6.3.4. O serviço deve prover disponibilidade de DNS 24x7x365, com nível de serviço de 99,999%;

1.6.3.5. O serviço deve ser provido por uma rede anycast distribuída nos pontos de presença descritos neste Termo de Referência;

1.6.3.6. A Plataforma deve prover mecanismos para aceleração de resolução de nomes DNS;

1.6.3.7. A solução deve implementar o serviço como DNS primário ou secundário, substituindo ou aumentando a infraestrutura DNS da SEF/MG;

1.6.3.8. A plataforma de DNS em nuvem deve prover:

1.6.3.8.1. Aceleração de resolução DNS;

1.6.3.8.2. Proteção contra ataques DNS;

1.6.3.8.3. Mecanismos que possibilitem a alta disponibilidade do serviço DNS;

1.6.3.8.4. Mecanismos para manutenção da configuração de DNS para os sítios a serem protegidos.

1.6.3.9. 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.

1.6.4. **Suporte Técnico**

1.6.4.1. O suporte técnico deve ser provido pela CONTRATADA e compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de erros, defeitos (*bugs*) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível de forma nativa na solução ou decorrente de qualquer adaptação (customização) e ajuste (tuning) efetuada pela SEF/MG, com atendimento 24 x 7 (vinte e quatro horas por dia, sete dias por semana).

1.6.4.2. O registro e o atendimento a um chamado de suporte técnico deverá ocorrer por qualquer uma das seguintes formas: contato telefônico, envio de mensagem eletrônica (e-mail), acesso ao sítio (*website*) da CONTRATADA ou do fabricante da solução, com controle de acesso por senha.

1.6.4.3. O atendimento telefônico, sempre que aplicável e viável, deverá ser realizado no idioma Português do Brasil, por meio de ligação local em Belo Horizonte/MG ou ligação interurbana gratuita (0800) e deverá ter um único número de contato para todos os produtos de *software* que compõem a solução.

1.6.4.4. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para a CONTRATADA, por qualquer uma das formas disponíveis, durante a vigência do contrato vinculado a este termo.

1.6.4.5. Na abertura ou registro de um chamado técnico, por qualquer uma das formas disponíveis, a CONTRATADA deverá informar: data e hora de abertura, descrição, nível de severidade do chamado e identificação completa do solicitante.

1.6.4.6. Cada chamado técnico será classificado em um dos 3 (três) níveis de severidade, descritos abaixo:

1.6.4.6.1. CRÍTICO: o problema causa perda ou paralisação total dos serviços da solução. O trabalho não pode ter sequência razoável, a operação passa a ser crítica para o negócio e a situação constitui uma emergência. O atendimento deverá ocorrer em até 4 (quatro) horas corridas da abertura do chamado pela CONTRATANTE.

1.6.4.6.2. MÉDIO: o problema causa uma grave perda de funcionalidade. Não está disponível nenhuma alternativa aceitável, mas as operações podem continuar ainda que de modo restrito. O atendimento deverá ocorrer em até 10 (dez) horas corridas da abertura do chamado pela CONTRATANTE.

1.6.4.6.3. NORMAL: o problema causa perda de funcionalidade de menor gravidade. O impacto constitui uma inconveniência, a qual pode requerer uma alternativa para restaurar a funcionalidade. O atendimento deverá ocorrer até o próximo dia útil da

abertura do chamado pela CONTRATANTE.

1.6.4.7. A CONTRATADA deverá retornar, via e-mail, a confirmação da abertura do chamado técnico, contemplando, ao menos, as seguintes informações: código de identificação do chamado, identificação do responsável da CONTRATADA e da CONTRATANTE pela abertura, nível de severidade do chamado e o problema relatado.

1.6.4.8. Um chamado técnico somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE, na forma de um visto na ordem de serviço correspondente ou aceite por e-mail ou diretamente no sistema disponibilizado pela CONTRATADA, caso esta forma seja utilizada.

1.6.4.9. Em caso de adoção de solução de contorno, sem prejuízo da solução definitiva cabível, a CONTRATADA deverá emitir laudos, na periodicidade exigida pela CONTRATANTE, informando sobre a evolução dos trabalhos para solucionar o problema de forma definitiva.

1.6.4.10. Após apresentar a solução definitiva para o chamado técnico, a CONTRATADA deverá retornar, via e-mail, a confirmação da execução do serviço, contemplando, ao menos, as seguintes informações: código de identificação do chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada, responsável pelo atendimento.

1.6.4.11. Deverá ser garantido à CONTRATANTE o pleno acesso ao sítio (site) do fabricante do produto que compõe a solução, com direito a consultas a quaisquer bases de conhecimentos e fóruns de discussão disponíveis aos usuários da solução.

1.6.4.12. A CONTRATADA deverá apresentar, para cada atualização de *software* disponível, a descrição de todas as modificações implementadas.

1.6.4.13. A CONTRATADA deverá atualizar os manuais correspondentes aos produtos, componentes ou módulos de *software*, sem ônus adicional à CONTRATANTE.

1.6.4.14. O prazo de atualização de todo *software* fornecido deverá ser igual ao período de garantia do produto. Durante a vigência do contrato, a CONTRATANTE terá direito a todas as atualizações de versão e *release* dos *software*.

1.6.4.15. Os *patches* e novas versões dos *software* integrantes da solução ofertada deverão ser instalados pela CONTRATADA tão logo estas se tornem disponíveis.

1.6.5. **Lote 1 - Item 4 - Serviços de instalação, configuração, teste em produção e ajuste.**

1.6.5.1. **Requisitos Gerais**

1.6.5.1.1. A configuração da solução será realizada pela CONTRATADA, com acompanhamento da equipe técnica da CONTRATANTE.

1.6.5.1.2. Para a execução dos serviços de instalação, configuração, testes em produção e ajustes, a CONTRATADA deverá alocar profissionais devidamente certificados pelo fabricante, para as tecnologias envolvidas ou o profissional do próprio fabricante da solução, tendo em vista a criticidade do ambiente.

1.6.5.1.3. A CONTRATADA deverá entregar à CONTRATANTE, em até (15) dias úteis, após o recebimento provisório da solução de segurança descrita no Lote 1 - itens 1 e 3, mídia digital no formato *Portable Document File* (PDF), contendo um rascunho do projeto da arquitetura e topologia, com as informações necessárias. Deverá ainda ser apresentado um Plano de Implantação da solução, contendo, no mínimo, os seguintes itens:

- Atividades a serem desempenhadas;
- Roteiro de implantação;
- Cronograma previsto para intervenção no ambiente da CONTRATANTE (a ser acordado com a CONTRATANTE), se aplicável;

- Responsáveis envolvidos nas fases de implantação e testes;
- Plano de retorno (*rollback*) em caso de falha na implantação, se aplicável.

1.6.5.1.4. A CONTRATADA deverá disponibilizar 1 (um) gerente de projeto responsável por acompanhar a instalação e configuração da solução. Esse profissional deverá, no mínimo:

- Fazer reunião de alinhamento e *overview* do escopo do projeto, gerenciamento de expectativas, planos de comunicação e requisitos necessários à implementação;
- Realizar a coleta de todas as informações necessárias para elaboração da arquitetura de implementação;
- Fazer a análise e definição da Arquitetura de Implementação, baseada nas melhores práticas de mercado, em conjunto com a equipe da CONTRATANTE;
- Analisar e mitigar riscos ao negócio;
- Estimar o impacto e janelas de indisponibilidade, se aplicável;
- Entregar a Arquitetura de Implementação para validação técnica da CONTRATANTE;
- Fornecer cronograma detalhado do projeto.

1.6.5.1.5. A CONTRATADA deverá configurar, instalar e testar os produtos, conforme projeto de implantação elaborado pela CONTRATADA e aprovado pela equipe técnica da CONTRATANTE, apresentando junto a cada produto um documento com instruções passo a passo para a instalação.

1.6.5.1.6. Os produtos fornecidos serão instalados e configurados em conformidade com o padrão da Rede da CONTRATANTE.

1.6.5.1.7. As ações de instalação, configuração e testes da solução serão realizadas pela CONTRATADA e deverão contemplar pelo menos as seguintes atividades:

- Análise preliminar da topologia e operação da Rede da CONTRATANTE com vistas a sua integração plena com a solução ofertada;
- Completa instalação e configuração, testes em produção e ajustes da solução ofertada;
- Implementação, com a coleta de evidências, dos controles de requisitos de segurança da CONTRATANTE, que forem possíveis de serem aplicados nos equipamentos/produtos da solução ofertada;
- Acompanhamento e homologação do ambiente de produção;
- Documentação detalhada de todos os passos da instalação, configuração e ajustes, no ambiente de produção, a qual deverá ser entregue em arquivo eletrônico no formato PDF, antes da emissão do Termo de Recebimento Definitivo a ser expedido pela CONTRATANTE.

1.6.5.1.8. Os trabalhos serão coordenados e acompanhados pelos analistas e técnicos da CONTRATANTE, devendo haver repasse de conhecimento durante a execução dos serviços.

1.6.5.1.9. A critério da CONTRATANTE, os serviços poderão ser executados fora do horário comercial e/ou em finais de semana ou feriados sem custo adicional para a CONTRATANTE, visando minimizar os transtornos aos usuários pela eventual indisponibilidade da rede.

1.6.5.1.10. Para todos os efeitos, a conclusão dos serviços de instalação, configuração, testes em produção e ajustes será dada pela entrega da solução em pleno funcionamento,

de acordo com as recomendações do(s) fabricante(s) e demais condições estabelecidas neste termo.

1.6.5.2. **Prazo de Execução**

1.6.5.2.1. O prazo total para a conclusão dos serviços de instalação, configuração, testes e documentação da solução não poderá ultrapassar 60 (sessenta) dias úteis, contados do início do serviço, salvo necessidade excepcional devidamente ajustada entre CONTRATANTE e CONTRATADA.

1.6.5.2.2. Um responsável técnico pelo projeto deverá estar disponível e acessível durante toda a fase de implantação, que deverá contemplar, no mínimo, as seguintes etapas:

1.6.5.2.2.1. Planejamento: nesta etapa a CONTRATADA deverá realizar o planejamento do projeto, em que serão definidos os prazos por atividade, as pessoas, a estratégia de implantação do serviço, o plano de testes, bem como quaisquer outros itens necessários à implantação do projeto. Deverão considerar as janelas de manutenção da CONTRATANTE, plano de *rollback* e o escopo definido. Os responsáveis técnicos designados pela CONTRATANTE acompanharão e aprovarão o planejamento.

1.6.5.2.2.2. Cronograma: a CONTRATADA deverá, em conjunto com representantes da Superintendência de Tecnologia e Informação (STI), elaborar e apresentar o cronograma detalhado, contendo todas as fases e datas previstas para disponibilizar a solução para uso, inclusive treinamentos, observados os prazos estabelecidos neste termo.

1.6.5.2.2.3. Plano de Implementação: a CONTRATADA, antes de iniciar a execução das configurações, deverá elaborar documentação técnica denominada “Plano de Implementação” detalhando e fundamentando todas as configurações que serão realizadas.

1.6.5.2.2.4. Plano de Testes: a CONTRATADA deverá entregar documentação técnica denominada “Plano de Testes” de forma a garantir que todas as características exigidas neste termo tenham sido satisfeitas. Deverá incluir no mínimo:

- Teste das funcionalidades da solução;
- Teste de alta disponibilidade;
- Teste de qualidade;
- Teste de desempenho.

1.6.5.2.3. Desde que solicitado pela CONTRATANTE, a CONTRATADA deverá fornecer um guia rápido de referência voltado aos usuários, customizado para utilização das principais funcionalidades da solução.

1.6.5.2.4. Toda a documentação será analisada pela CONTRATANTE e deverá ser complementada pela CONTRATADA, caso seja solicitado.

1.6.5.2.5. Após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas e o cumprimento dos prazos pactuados.

1.6.5.2.6. A implantação deverá ocorrer conforme planejamento realizado e segundo as diretrizes da CONTRATANTE.

1.6.5.2.7. Finalização: a solução implantada será aceita, se e somente se, houver comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos. Essa comprovação será feita mediante observação direta das características dos componentes da solução, o funcionamento adequado das funções especificadas, consulta à documentação técnica fornecida e verificação dos

serviços de instalação e configuração, além da realização da Prova de Conceito.

1.6.5.2.8. Documentação Final: após a implementação, a CONTRATADA deverá entregar a documentação técnica final do projeto, contendo, no mínimo, a implementação realizada, arquitetura adotada, descrição e forma da redundância, instruções para *backup*/restauração, cópia das configurações realizadas em todos os elementos com comentários, número serial dos produtos entregues, lista de material dos produtos entregues. Deverá incluir outras informações que a CONTRATANTE ou a CONTRATADA julgarem importantes para o registro fiel de como a solução foi implementada. Essa documentação será denominada Documentação Final.

1.6.5.2.9. O Termo de Recebimento Definitivo da solução descrita no Lote 1 - itens 1 e 3 deste Termo de Referência será emitido e entregue à CONTRATADA após a finalização dos serviços de instalação, configuração e testes.

1.6.5.3. **Repasse de Conhecimento:**

1.6.5.3.1. Repasse de conhecimento da solução ofertada no Lote 1 - itens 1 e 3, tipo teórico e prático.

1.6.5.3.2. O(s) instrutor(es) deverá(ão) possuir conhecimento comprovado da solução fornecida.

1.6.5.3.3. Deverá ser realizado no ambiente da CONTRATANTE ou de forma on line, com aulas ao vivo e com material didático digital (PPT ou PDF, documentação do projeto e manuais de produto) fornecido pela CONTRATADA.

1.6.5.3.3.1. O repasse de conhecimento poderá ser gravado pela CONTRATANTE.

1.6.5.3.4. O repasse de conhecimento deverá ser realizado pela CONTRATADA para uma turma de 6 (seis) vagas, para analistas e técnicos da CONTRATANTE e deverá ser ministrado no turno matutino ou vespertino, conforme a necessidade da SEF/MG, em horário comercial e dias úteis.

1.6.5.3.5. O repasse de conhecimento compreenderá necessariamente os seguintes tópicos:

1.6.5.3.5.1. Instalação, configuração e operação do produto;

1.6.5.3.5.2. Apresentação do projeto da CONTRATANTE;

1.6.5.3.5.3. Descrição da arquitetura do produto;

1.6.5.3.5.4. Descrição dos *software* disponíveis no produto;

1.6.5.3.5.5. Estratégias de implementação do produto.

1.6.5.3.6. É responsabilidade da CONTRATANTE zelar pelo comparecimento e assiduidade dos servidores/analistas à capacitação aplicada.

1.6.5.3.7. A CONTRATANTE poderá solicitar a repetição do repasse de conhecimento caso entenda que o mesmo não cumpriu os requisitos estabelecidos.

1.6.5.3.8. O repasse de conhecimento não se confunde com o treinamento previsto para a solução.

1.6.6. **Lote 1 - Item 5 - Treinamento**

1.6.6.1. Treinamento completo da solução ofertada no Lote 1 - itens 1 e 3 do tipo teórico e prático.

1.6.6.2. Os instrutores deverão ser certificados pelo fabricante e possuir conhecimentos comprovados na solução fornecida.

1.6.6.3. A CONTRATADA deverá apresentar, quando da execução do contrato, certidão de capacidade técnica e documento comprobatório de parceria com o fabricante do produto e autorização para ministrar o treinamento oficial. Será aceito o fornecimento de treinamento

oficial por meio da contratação de centro de treinamentos autorizado pelo fabricante.

1.6.6.4. A CONTRATADA disponibilizará laboratório que permita a simulação de ambientes com características similares aos propostos na solução implantada, possibilitando exercícios práticos de configuração do produto durante os módulos de capacitação em que tais atividades se apliquem. O ambiente de laboratório poderá ser montado em local disponibilizado pela CONTRATADA, em Belo Horizonte/MG, ou poderá estar nas dependências do fabricante e/ou fornecedor. Caso o laboratório esteja nas dependências do fabricante e/ou fornecedor, deverá ser acessado por meio de VPN/Internet, durante o período do treinamento, sendo de responsabilidade da CONTRATADA a disponibilização de local, em Belo Horizonte/MG, para realização do treinamento, bem como o acesso ao laboratório do fabricante e/ou fornecedor, com todos os recursos necessários (espaço físico, equipamentos, material didático, entre outros).

1.6.6.4.1. **Mediante formalização por parte da CONTRATADA, a CONTRATANTE poderá avaliar e aceitar que o treinamento seja feito de forma virtual. Nesse contexto, os técnicos a serem treinados deverão ter acesso à plataforma de treinamento do fornecedor ou do fabricante, mantendo-se as demais condições definidas nesta especificação**.

1.6.6.5. Em caso de treinamento presencial, o local deverá ser disponibilizado pela CONTRATADA na cidade de Belo Horizonte, devendo todos os custos (sala, instrutores, desktop, dentre outros) serem de responsabilidade da CONTRATADA.

1.6.6.6. Em caso de treinamento *on line*, as aulas deverão ser ao vivo e ministradas em língua portuguesa. Faculta-se à CONTRATANTE o direito de gravar as aulas.

1.6.6.7. O treinamento deverá ser realizado pela CONTRATADA, **em 1 (uma) turma de 6 (seis) vagas**, para analistas e técnicos da CONTRATANTE, perfazendo o total de horas/aula recomendado pelo fabricante da solução.

1.6.6.8. O treinamento estará centrado na solução fornecida, privilegiando atividades práticas que permitam melhor fixação do aprendizado, de forma a possibilitar à equipe técnica da CONTRATANTE gerenciar e administrar a solução implantada.

1.6.6.9. A CONTRATADA deverá fornecer, no início de cada tópico, apostilas (em formato impresso ou digital) que abordem todo o conteúdo programático, as quais poderão estar no todo ou em parte, em português e/ou inglês. O conteúdo do treinamento deverá abranger, pelo menos, os seguintes tópicos: instalação, configuração, operação, monitoramento, administração básica e avançada, relatórios.

1.6.6.10. O início dessa atividade, bem como o período e horário de realização, serão definidos pela CONTRATANTE em comum acordo com a CONTRATADA.

1.6.6.11. É responsabilidade da CONTRATANTE zelar pelo comparecimento e assiduidade dos treinandos à capacitação aplicada.

1.6.6.12. Ao final do treinamento deverá ser emitido certificado de conclusão para cada participante/aluno constando a carga horária e a ementa.

1.6.6.13. A CONTRATANTE poderá solicitar a repetição do treinamento caso entenda que o mesmo não cumpriu os requisitos estabelecidos.

1.6.7. **Lote 2 - Item 1 - Solução Security Service Edge (SSE)**

1.6.7.1. **Características Gerais**

1.6.7.1.1. A solução deve ser entregue em uma plataforma integrada do fabricante, permitindo a navegação entre as tecnologias por meio de console única. Considera-se composição a existência de gerenciamento segregado e a necessidade de login em solução de terceiros.

1.6.7.1.2. A solução de SSE deve fornecer os seguintes recursos:

1.6.7.1.2.1. FWaaS (Firewall as a Service);

1.6.7.1.2.2. ZTNA (Zero Trust Network Access);

1.6.7.1.2.3. SWG (Secure Web Gateway);

1.6.7.1.2.4. RBI (Remote Browser Isolation);

1.6.7.1.2.5. CASB (Cloud Access Security Broker);

1.6.7.1.2.6. DLP (Data Loss Prevention);

1.6.7.1.3. A solução deve ser entregue com as licenças necessárias para atendimento de todos os itens deste termo de referência;

1.6.7.1.4. A solução deve ser licenciada por usuário, por volume de tráfego/largura de banda, número de dispositivos, de acordo com o padrão adotado pelo fabricante;

1.6.7.1.5. A solução deve ser baseada em nuvem, unificando e aprimorando a proteção do acesso a aplicações, dados e usuário, independentemente da localização;

1.6.7.1.6. A solução deve ter ao menos um ponto de presença no Brasil;

1.6.7.1.7. A solução deve permitir e estar licenciada para provisionamento em, no mínimo, 4 (quatro) pontos de presença (POP);

1.6.7.1.7.1. Os 4 (quatro) pontos de presença incluídos na solução devem permitir a configuração de, no mínimo, 1 (um) endereço IP fixo para cada. Caso a solução exija licenciamento adicional, este deve ser entregue para todos os POPs;

1.6.7.1.8. A solução deve possuir, além da redundância geográfica, a possibilidade da SEF/MG escolher em qual POP os logs serão armazenados para estar em compliance com legislações locais;

1.6.7.1.9. O acesso à console de administração da solução SSE deve ser feito via navegador web e ter a possibilidade de se integrar com IdP para autenticação SSO dos usuários administrativos;

1.6.7.1.10. A solução deve permitir a criação de políticas de acesso baseadas em contexto, como localização geográfica e horário;

1.6.7.1.11. A solução deve oferecer logs detalhados de tentativas de autenticação, incluindo localização, dispositivo e risco de acesso;

1.6.7.1.12. A solução deve garantir o acesso seguro à web, serviços em nuvem e aplicações privadas, independentemente da localização do usuário ou de onde essas aplicações estão hospedadas;

1.6.7.1.13. A solução deve fornecer proteção contra ameaças à rede em tempo real, atuando sobre o tráfego originado no dispositivo do usuário com destino às aplicações e serviços de internet;

1.6.7.1.14. A solução deve estar em conformidade com as regulamentações e padrões de segurança relevantes, como a Lei Geral de Proteção de Dados Pessoais (LGPD);

1.6.7.1.15. A solução deve ser monitorada e gerenciada 24 (vinte e quatro) horas por dia, 07 (sete) dias por semanas, com disponibilidade mensal de 99.999% para todos os serviços;

1.6.7.1.16. A solução deve possuir proteção contra ataques cibernéticos, visando a disponibilidade do acesso ao serviço;

1.6.7.1.17. A comunicação entre agentes (clientes) e outras soluções de infraestrutura SSE devem sempre usar comunicação segura criptografada;

1.6.7.1.18. A solução deve entregar tenant exclusivo e isolado, evitando que os dados possam ser acessados por outros tenants, mantendo o sigilo da informação, com acesso via internet e por conexão;

1.6.7.1.19. O fabricante deve possuir ao menos uma das seguintes certificações de compliance: SOC 2 Tipo 2, ISO 27001, ISO 27701 ou ISO 27018.

1.6.7.1.20. A solução deve utilizar agente único para todas as suas funcionalidades;

1.6.7.1.20.1. O agente único deverá ser compatível com os Sistemas Operacionais: MacOS, Windows, Linux, IOS e Android.

1.6.7.1.20.2. A solução deve utilizar o mesmo agente para acessos à infraestrutura interna e externa da secretaria.

1.6.7.2. **Zero Trust Network Access**

1.6.7.2.1. A solução deve atender a políticas de permissão e negação de acesso com base, no mínimo, nas seguintes condições condições: Postura do Dispositivo, Localização do Dispositivo/Usuário e Associação ao Grupo de Usuários;

1.6.7.2.2. A solução deve possuir capacidade de analisar os acessos dos usuários remotos às aplicações na infraestrutura interna da Secretaria de Estado de Fazenda de Minas Gerais (SEF/MG);

1.6.7.2.3. A solução deve possuir capacidade de controlar o acesso de usuários remotos a aplicações internas da SEF/MG, por meio da nuvem do fabricante, de modo que o usuário remoto tenha acesso apenas à aplicação especificada e não a um segmento de rede interna;

1.6.7.2.4. A solução deve ser autossuficiente e se ajustar automaticamente do ponto de vista de performance, caso algum ponto de presença venha a falhar, sem a necessidade do administrador ou cliente configurar qualquer regra;

1.6.7.2.5. A solução deve possuir, no mínimo, as seguintes funcionalidades: Antimalware, Sandboxing, controle de acesso URL;

1.6.7.2.6. A solução deve prover serviços de maneira transparente aos usuários remotos;

1.6.7.2.7. O ZTNA não deve ter acesso e nem ser atribuído a um segmento de rede interna como ocorre com a Virtual Private Network (VPN);

1.6.7.2.8. A solução deve prover acesso a aplicações internas específicas, via browser, sem agente para usuários remotos com dispositivos não gerenciados;

1.6.7.2.8.1. O acesso sem agente deverá promover conexão segura ao portal da solução, o qual proverá controle de tráfego para as aplicações internet, SaaS e internas;

1.6.7.2.8.2. O agente deverá se comunicar com o portal para determinar as políticas de segurança do usuário;

1.6.7.2.9. A solução deve possibilitar a execução de políticas de segurança das seguintes formas:

1.6.7.2.9.1. Antes da conexão com a SEF/MG (verificação de compliance);

1.6.7.2.9.2. Após autenticação do usuário na estação;

1.6.7.2.9.3. Sob demanda da secretaria;

1.6.7.2.10. A solução deve manter conexão segura com o portal durante a sessão;

1.6.7.2.11. A solução deve bloquear ou quarentenar usuários por perfis de acesso e grupo de ativos, quando esses não atenderem às políticas de segurança;

1.6.7.2.12. A solução deve possuir mecanismos de checagem de conformidade do dispositivo remoto;

1.6.7.2.13. A solução deve verificar, no mínimo, as seguintes informações no cliente remoto: Sistema Operacional, Processos Ativos, Antimalware e versão instalada;

1.6.7.2.14. A solução deve assegurar que a conformidade seja mantida de maneira contínua durante a conexão, mudando o status para "Não compliance", caso seja detectada não conformidade;

1.6.7.2.15. A solução deve prover a conexão entre a solução e a infraestrutura da

SEF/MG, permitindo que os usuários remotos acessem as Aplicações/Serviços instalados na infraestrutura da secretaria;

1.6.7.2.16. A solução deve prover a criação de conexões seguras para garantir a confidencialidade dos dados em trânsito entre a Solução e a infraestrutura da SEF/MG;

1.6.7.2.17. A solução deve prover a configuração de um portal para acesso às aplicações internas sem a necessidade de agente instalado na máquina do usuário.

1.6.7.2.17.1. No caso de acesso sem o uso de agentes, o IdP (Identity Provider) deverá ser utilizado para validar a identidade do usuário antes de fornecer qualquer tipo de conectividade via Proxy Reverso, ou similar, com a aplicação Web privada;

1.6.7.2.18. O portal para acesso às aplicações internas, sem a necessidade de um agente instalado na máquina do usuário, deve suportar a configuração de no mínimo:

1.6.7.2.18.1. Aplicações WEB (HTTP e HTTPS);

1.6.7.2.18.2. RDP;

1.6.7.2.18.3. SSH;

1.6.7.2.19. A solução deve suportar a integração com aplicações SaaS e on-premises;

1.6.7.2.20. A solução deve permitir a adição de aplicações web autogerenciadas, configurando-as como aplicações self-hosted;

1.6.7.2.21. A solução deve oferecer integração com aplicações de infraestrutura, permitindo o controle de acesso a servidores SSH, bancos de dados e outros serviços não HTTP;

1.6.7.2.22. A solução deve permitir a publicação segura de aplicações autogerenciadas na Internet, utilizando mecanismos de conexão segura entre o servidor de origem e a rede protegida.

1.6.7.2.23. A solução deve possibilitar a aplicação de políticas de segurança específicas para cada aplicação.

1.6.7.2.24. A solução deve permitir a configuração de páginas de login personalizadas para aplicações protegidas.

1.6.7.2.25. A solução deve permitir a configuração de páginas de bloqueio personalizadas para acessos não autorizados.

1.6.7.3. **Secure Web Gateway - SWG**

1.6.7.3.1. A solução deve suportar a implementação de Secure Web Gateway (SWG) para controle e proteção do tráfego de internet;

1.6.7.3.2. A solução deve ser responsável pela visibilidade e controle do tráfego por camada de aplicação de forma granular;

1.6.7.3.3. A solução deve permitir a criação de listas customizadas para filtragem web, incluindo bloqueio e permissão por, no mínimo:

1.6.7.3.3.1. URL;

1.6.7.3.3.2. Categoria;

1.6.7.3.3.3. Domínio;

1.6.7.3.3.4. IP;

1.6.7.3.4. A solução deve prover visibilidade e controle em tempo real de acesso a URLs, por meio de classificação baseada em categorias;

1.6.7.3.5. A solução deve ser responsável pela visibilidade e controle do tráfego corporativo em direção ao Microsoft Office 365, em tempo real a partir de estações de trabalho com agente ou via RBI;

1.6.7.3.6. A solução deve prevenir e restringir acesso a sites maliciosos;

1.6.7.3.7. A solução deve prevenir contra download de artefatos maliciosos;

1.6.7.3.8. A solução deve ser compatível com as plataformas Windows, MacOS, Linux, Android e IOS;

1.6.7.3.9. A solução deve permitir aplicar ação de bloqueio para contas pessoais e corporativas do Microsoft Office 365 e demais aplicações SaaS;

1.6.7.3.10. A solução deve permitir a criação de regras para acesso à plataforma do Office 365 Corporativo;

1.6.7.3.11. A solução deve oferecer políticas para inspecionar tráfego DNS, de rede, HTTP e de saída, permitindo o bloqueio de domínios e endereços IP maliciosos;

1.6.7.3.12. A solução deve realizar inspeção de SSL/TLS em 100% do tráfego Web, sem limites de volume de transações ou percentual inspecionado, em protocolos TLS 1.2 e superior;

1.6.7.3.13. A solução deve permitir a criação de regras granulares de exceção à inspeção SSL/TLS, com base nas categorias de URL, hosts e domínios de destino, usuário, grupo, ou tipo de browsers;

1.6.7.3.14. A solução deve permitir a configuração de políticas de isolamento de navegador, garantindo que o tráfego seja renderizado em um navegador isolado para proteger contra ameaças da web, possuindo os seguintes requisitos:

1.6.7.3.14.1. Implementar a funcionalidade RBI de forma transparente aos usuários, sem necessidade de alteração de configurações no navegador e sem necessidade de instalação de plugins, além de não provocar impacto significativo no desempenho do site/experiência do usuário do site acessado;

1.6.7.3.14.2. Possibilitar a configuração de forma seletiva (site, domínio, web app), para acessar sites relacionados a novos domínios ou ainda potencialmente maliciosos, de forma isolada e restrita, protegendo o dispositivo do usuário de possíveis ameaças;

1.6.7.3.14.3. Ser compatível com os principais navegadores de mercado como, por exemplo: Google Chrome, Safari, Firefox e Microsoft Edge;

1.6.7.3.14.4. Efetuar a identificação precisa de usuários por meio dos agentes da solução. Para os casos de tráfego associado a usuários em equipamentos sem agente na rede corporativa, a solução deve possibilitar alternativas de rastreabilidade, como a integração com Microsoft AD e Entra ID via SAML;

1.6.7.3.15. A solução deve permitir a aplicação de políticas baseadas na identidade do usuário, utilizando seletores de identidade para filtrar o tráfego de saída;

1.6.7.3.16. A solução deve fornecer logs detalhados e recursos de monitoramento para análise e auditoria;

1.6.7.3.17. A solução deve oferecer autenticação integrada para assegurar que apenas usuários autorizados acessem a internet;

1.6.7.3.18. A solução deve fornecer relatórios detalhados sobre o uso da web e incidentes de segurança;

1.6.7.3.19. A solução deve suportar a análise e controle de tráfego de aplicativos em tempo real;

1.6.7.3.20. A solução deve permitir a configuração de políticas baseadas em identidade do usuário e grupos;

1.6.7.3.21. A solução deve permitir a inspeção de tráfego de aplicações SaaS, fornecendo controle sobre uso de ferramentas não autorizadas;

1.6.7.3.22. A solução deve permitir o controle de acesso a categorias não autorizadas, que imponham risco à segurança, como Botnets, Domain Generation Algorithms (DGA),

Command & Control, Sites Maliciosos e Phishing e a sites restritos, como Pornografia, Drogas, Atividades Criminais e Apostas;

1.6.7.3.23. A solução deve possibilitar o bloqueio dinâmico de domínios recém-criados ou suspeitos;

1.6.7.3.24. A solução deve permitir a segmentação de tráfego por perfil de risco para definir níveis diferenciados de acesso e proteção;

1.6.7.4. **Cloud Access Security Broker (CASB)**

1.6.7.4.1. A solução deve possuir funcionalidades de SSPM (SaaS Security Posture Management – Gerenciamento de postura de segurança SaaS) com a finalidade de identificar, monitorar de forma contínua, categorizar automaticamente aplicações de nuvem em uso (Gerenciadas ou não-gerenciadas), considerando múltiplos critérios de segurança, como postura e compliance;

1.6.7.4.2. A solução deve permitir o bloqueio de aplicações não gerenciadas, para classificação da reputação, contemplando parâmetros, tais como:

1.6.7.4.2.1. Categoria da aplicação;

1.6.7.4.2.2. Configurações inseguras;

1.6.7.4.2.3. Duplo fator de autenticação (MFA) habilitado;

1.6.7.4.2.4. Mecanismos de criptografia;

1.6.7.4.2.5. Score de risco;

1.6.7.4.2.6. Shadow IT (Uso de software não autorizado);

1.6.7.4.3. A solução deve permitir a configuração de quais aplicações SaaS devem ter a inspeção do túnel TLS ativada;

1.6.7.4.4. A solução deve possuir relatório com métricas de utilização dos usuários, atividades e volume de tráfego;

1.6.7.4.5. A solução deve identificar o uso de aplicações não autorizadas e com risco elevado, além de visualização dos usuários que estão utilizando essas aplicações, permitindo ações de mitigação, tais como:

1.6.7.4.5.1. Auditoria;

1.6.7.4.5.2. Cancelar compartilhamento para todos;

1.6.7.4.5.3. Cancelar compartilhamento para usuários externos;

1.6.7.4.5.4. Cancelar compartilhamento para usuários Internos;

1.6.7.4.5.5. Quarentena

1.6.7.4.6. A solução deve prover mecanismos de chamada a sistemas externos por meio de APIs Rest, para automação de processos de notificação, alertas e controle de acesso;

1.6.7.4.7. A solução deve possuir técnicas de monitoração quanto à exposição de dados na internet, identificando ameaças e permitindo criar políticas de segurança automatizadas;

1.6.7.4.8. A solução deve possuir suporte as principais aplicações SaaS hospedadas em infraestrutura de nuvem pública como Azure, AWS e Google, permitindo o registro e monitoramento de todas as atividades do usuário;

1.6.7.4.9. A solução deve possuir alertas de malicious insiders (acesso suspeito de dados), como, por exemplo, alta quantidade de download em curto espaço de tempo;

1.6.7.4.10. A solução deve possuir análise de comportamento de usuários automática para detecção de utilização anômala e comportamento suspeito;

1.6.7.4.11. A solução deve possuir controle de políticas de acesso customizadas para

controle de Bring Your Own Device (BYOD) e dispositivos corporativos;

1.6.7.4.12. A solução deve permitir controlar download e upload de arquivos;

1.6.7.4.13. A solução deve executar conexão/integração direta por API para 3500 (três mil e quinhentos) usuários com a Suíte O365 (OneDrive, Outlook, Sharepoint e Teams);

1.6.7.4.14. A solução deve permitir criar políticas que revoguem o acesso à determinada aplicação terceira;

1.6.7.4.15. A solução deve permitir monitorar todas as atividades de usuários pré-selecionados;

1.6.7.4.16. A solução deve detectar anomalias e identificar padrões indicativos de atividade maliciosa;

1.6.7.4.17. A solução deve proteger:

1.6.7.4.17.1. contra malwares;

1.6.7.4.17.2. contra sequestro de conta ou sessão;

1.6.7.4.18. A solução deve oferecer controle de acesso granular contextual ou por políticas, com base em variedade de fatores, tais como, dispositivo, localização e atividade;

1.6.7.4.19. A solução deve executar ações de análise de comportamento da entidade do usuário (UEBA), visando a detecção de ameaças internas e contas comprometidas;

1.6.7.5. **Data Loss Prevention**

1.6.7.5.1. A solução deve suportar a inspeção e análise avançada de tráfego para identificar padrões de exfiltração de dados;

1.6.7.5.2. A solução deve suportar a integração com APIs para controle de dados em aplicações de terceiros;

1.6.7.5.3. A solução deve suportar a prevenção de compartilhamento não autorizado de dados entre ambientes de nuvem distintos;

1.6.7.5.4. A solução deve suportar políticas de DLP para identificação de padrões como expressões regulares, OCR e fingerprinting de documentos;

1.6.7.5.5. A solução deve suportar a análise de tráfego HTTP e HTTPS para detecção de dados sensíveis em tempo real;

1.6.7.5.6. A solução deve permitir a configuração de ações automáticas para bloqueio e alerta;

1.6.7.5.7. A solução deve permitir a aplicação de políticas de DLP com base no perfil do usuário, grupo ou área de negócio;

1.6.7.5.8. A solução deve oferecer relatórios detalhados sobre incidentes de DLP, fornecendo visibilidade completa das violações e ações tomadas;

1.6.7.5.9. A solução deve permitir a configuração de listas de permitidos e bloqueados para controle de informações confidenciais compartilhadas;

1.6.7.5.10. A solução deve possibilitar a análise de padrões de transferência de dados para detectar atividades anômalas e suspeitas;

1.6.7.5.11. A solução deve oferecer a capacidade de aplicar políticas granulares para diferentes tipos de dados;

1.6.7.5.12. A solução deve suportar a conformidade com regulamentações como GDPR, LGPD e outras normas de proteção de dados;

1.6.7.5.13. A solução deve permitir auditoria e rastreamento de eventos de DLP para investigações forenses e conformidade regulatória;

1.6.7.5.14. A solução deve suportar a criação de regras específicas para evitar o envio

não autorizado de informações confidenciais por e-mail e outros canais de comunicação;

1.6.7.5.15. A solução deve suportar a exportação e compartilhamento de logs de DLP para ferramentas de análise e correlação de eventos de segurança;

1.6.7.6. **Monitoramento de Logs**

1.6.7.6.1. A solução deve oferecer alertas automáticos para anomalias de segurança e tentativas de acesso não autorizadas;

1.6.7.6.2. A solução deve suportar logs detalhados para integração com ferramentas externas;

1.6.7.6.3. A solução deve permitir armazenamento seguro dos logs em conformidade com regulamentações como LGPD e GDPR;

1.6.7.6.4. A solução deve suportar auditoria detalhada de eventos de acesso, incluindo logs de autenticação e ações executadas;

1.6.7.6.5. A solução deve permitir exportação automatizada de logs para plataformas SIEM;

1.6.7.6.6. A solução deve suportar retenção de logs por períodos configuráveis para conformidade regulatória;

1.6.7.6.7. A solução deve permitir segmentação de logs por usuário, dispositivo e aplicação acessada;

1.6.7.6.8. A solução deve suportar registros de tentativas de acesso bloqueadas e motivos da rejeição;

1.6.7.6.9. A solução deve oferecer APIs para acesso aos logs e eventos de monitoramento;

1.6.7.7. **Gerenciamento de Políticas**

1.6.7.7.1. A solução deve suportar a criação e a gestão centralizada de políticas de acesso.

1.6.7.7.2. A solução deve permitir a definição de políticas com base em identidade, localização e postura do dispositivo.

1.6.7.7.3. A solução deve oferecer mecanismo de atualização dinâmica de políticas com base em inteligência de ameaças.

1.6.7.7.4. A solução deve possibilitar a configuração de ações específicas (permitir, bloquear, bypass, autenticação de serviço) dentro das políticas de acesso.

1.6.7.7.5. A solução deve suportar a definição de regras de inclusão, exclusão e requisitos dentro das políticas, permitindo o controle granular sobre quem pode acessar quais recursos.

1.6.7.7.6. A solução deve permitir a utilização de seletores variados, como identidade do usuário, grupos, endereços IP, países e métodos de autenticação, para a construção de políticas robustas.

1.6.7.7.7. A solução deve permitir que as políticas sejam avaliadas em uma ordem específica, permitindo a priorização de regras conforme necessário.

1.6.7.7.8. A solução deve fornecer mecanismos para evitar configurações incorretas comuns, como a inclusão inadvertida de todos os usuários em uma política.

1.6.7.7.9. A solução deve permitir a integração com APIs externas para validação personalizada durante a avaliação das políticas de acesso.

1.6.7.7.10. A solução deve oferecer suporte a políticas de acesso extensíveis, permitindo chamadas a qualquer API durante a avaliação de uma política.

1.6.7.7.11. A solução deve permitir a aplicação de políticas de acesso baseadas em

contexto e com privilégios mínimos para cada recurso, reduzindo a superfície de ataque e eliminando movimentos laterais.

1.6.7.7.12. A solução deve possibilitar a autenticação de usuários terceirizados (como prestadores de serviços) com opções sem cliente, provedores de identidade, dentre outros métodos.

1.6.7.7.13. A solução deve permitir a implementação de políticas de segurança Zero Trust, garantindo que nenhuma solicitação seja confiável por padrão e que todas sejam verificadas rigorosamente.

1.6.7.7.14. A solução deve fornecer ferramentas para monitoramento e validação contínuos das políticas de acesso implementadas, garantindo conformidade e segurança contínuas.

1.6.7.7.15. A solução deve permitir a aplicação do princípio do menor privilégio, garantindo que os usuários tenham apenas o acesso necessário para desempenhar suas funções.

1.6.7.8. **Consultas e Relatórios**

1.6.7.8.1. A solução deve possuir opção para gerar relatórios a partir dos dados monitorados;

1.6.7.8.2. A solução deve possibilitar a visualização dos eventos contextualizados e ocorridos no passado (base histórica), possibilitando investigação dos incidentes e suas causas raízes;

1.6.7.8.3. A solução deve disponibilizar todo o ciclo de execução de processos suspeitos, com a opção de visualizar os dados relevantes à análise dos incidentes, com a opção de filtros de buscas;

1.6.7.8.4. A solução deve demonstrar na forma de linha do tempo todos os passos da execução das atividades consideradas suspeitas;

1.6.7.8.5. A solução deve monitorar a experiência do usuário quanto a latência e disponibilidade das aplicações que interagem com a infraestrutura da SEF/MG;

1.6.7.9. **Suporte Técnico**

1.6.7.9.1. O suporte técnico deve ser provido pela CONTRATADA e compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de erros, defeitos (*bugs*) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível de forma nativa na solução ou decorrente de qualquer adaptação (customização) e ajuste (tuning) efetuada pela SEF/MG, com atendimento 24 x 7 (vinte e quatro horas por dia, sete dias por semana).

1.6.7.9.2. O registro e o atendimento ao chamado de suporte técnico deverá ocorrer por qualquer uma das seguintes formas: contato telefônico, envio de mensagem eletrônica (e-mail), acesso ao sítio (*website*) da CONTRATADA ou do fabricante da solução, com controle de acesso por senha.

1.6.7.9.3. O atendimento telefônico, sempre que aplicável e viável, deverá ser realizado no idioma Português do Brasil, por meio de ligação local em Belo Horizonte/MG ou ligação interurbana gratuita (0800) e deverá ter um único número de contato para todos os produtos de *software* que compõem a solução.

1.6.7.9.4. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para a CONTRATADA, por qualquer uma das formas disponíveis, durante a vigência do contrato vinculado a este termo.

1.6.7.9.5. Na abertura ou registro de um chamado técnico, por qualquer uma das formas disponíveis, a CONTRATADA deverá informar: data e hora de abertura, descrição, nível de severidade do chamado e identificação completa do solicitante.

1.6.7.9.6. Cada chamado técnico será classificado em um dos 3 (três) níveis de

severidade, descritos abaixo:

1.6.7.9.6.1. CRÍTICO: o problema causa perda ou paralisação total dos serviços da solução. O trabalho não pode ter sequência razoável, a operação passa a ser crítica para o negócio e a situação constitui uma emergência. O atendimento deverá ocorrer em até 4 (quatro) horas corridas da abertura do chamado pela CONTRATANTE.

1.6.7.9.6.2. MÉDIO: o problema causa grave perda de funcionalidade. Não está disponível nenhuma alternativa aceitável, mas as operações podem continuar ainda que de modo restrito. O atendimento deverá ocorrer em até 10 (dez) horas corridas da abertura do chamado pela CONTRATANTE.

1.6.7.9.6.3. NORMAL: o problema causa perda de funcionalidade de menor gravidade. O impacto constitui uma inconveniência, a qual pode requerer uma alternativa para restaurar a funcionalidade. O atendimento deverá ocorrer até o próximo dia útil da abertura do chamado pela CONTRATANTE.

1.6.7.9.7. A CONTRATADA deverá retornar, via e-mail, a confirmação da abertura do chamado técnico, contemplando, ao menos, as seguintes informações: código de identificação do chamado, identificação do responsável da CONTRATADA e da CONTRATANTE pela abertura, nível de severidade do chamado e o problema relatado.

1.6.7.9.8. O chamado técnico somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE, na forma de um visto na ordem de serviço correspondente ou aceite por e-mail ou diretamente no sistema disponibilizado pela CONTRATADA, caso esta forma seja utilizada.

1.6.7.9.9. Em caso de adoção de solução de contorno, sem prejuízo da solução definitiva cabível, a CONTRATADA deverá emitir laudos, na periodicidade exigida pela CONTRATANTE, informando sobre a evolução dos trabalhos para solucionar o problema de forma definitiva.

1.6.7.9.10. Após apresentar a solução definitiva para o chamado técnico, a CONTRATADA deverá retornar, via e-mail, a confirmação da execução do serviço, contemplando, ao menos, as seguintes informações: código de identificação do chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada, responsável pelo atendimento.

1.6.7.9.11. Deverá ser garantido à CONTRATANTE o pleno acesso ao sítio (site) do fabricante do produto que compõe a solução, com direito a consultas a quaisquer bases de conhecimentos e fóruns de discussão disponíveis aos usuários da solução.

1.6.7.9.12. A CONTRATADA deverá apresentar, para cada atualização de *software* disponível, a descrição de todas as modificações implementadas.

1.6.7.9.13. A CONTRATADA deverá atualizar os manuais correspondentes aos produtos, componentes ou módulos de *software*, sem ônus adicional à CONTRATANTE.

1.6.7.9.14. O prazo de atualização de todo *software* fornecido deverá ser igual ao período de garantia do produto. Durante a vigência do contrato, a CONTRATANTE terá direito a todas as atualizações de versão e *release* dos *software*.

1.6.7.9.15. Os *patches* e novas versões dos *software* integrantes da solução ofertada deverão ser instalados pela CONTRATADA tão logo estas se tornem disponíveis.

1.6.8. **Lote 2 - Item 2 - Serviços de instalação, configuração, testes em produção, ajustes dos equipamentos/produtos da solução**

1.6.8.1. **Requisitos Gerais**

1.6.8.1.1. A configuração da solução será realizada pela CONTRATADA, com acompanhamento da equipe técnica da CONTRATANTE.

1.6.8.1.2. Para a execução dos serviços de instalação, configuração, testes em

produção e ajustes, a CONTRATADA deverá alocar profissionais devidamente certificados pelo fabricante, para as tecnologias envolvidas ou o profissional do próprio fabricante da solução, tendo em vista a criticidade do ambiente.

1.6.8.1.3. A CONTRATADA deverá entregar à CONTRATANTE, em até (15) dias úteis, após o recebimento provisório da solução de segurança descrita no Lote 2 - item 1, mídia digital no formato *Portable Document File* (PDF), contendo o rascunho do projeto da arquitetura e topologia, com as informações necessárias. Deverá ainda ser apresentado o Plano de Implantação da solução, contendo, no mínimo, os seguintes itens:

- Atividades a serem desempenhadas;
- Roteiro de implantação;
- Cronograma previsto para intervenção no ambiente da CONTRATANTE (a ser acordado com a CONTRATANTE), se aplicável;
- Responsáveis envolvidos nas fases de implantação e testes;
- Plano de retorno (*rollback*) em caso de falha na implantação, se aplicável.

1.6.8.1.4. A CONTRATADA deverá disponibilizar 1 (um) gerente de projeto responsável por acompanhar a instalação e configuração da solução. Esse profissional deverá, no mínimo:

- Fazer reunião de alinhamento e *overview* do escopo do projeto, gerenciamento de expectativas, planos de comunicação e requisitos necessários à implementação;
- Realizar a coleta de todas as informações necessárias para elaboração da arquitetura de implementação;
- Fazer a análise e definição da Arquitetura de Implementação, baseada nas melhores práticas de mercado, em conjunto com a equipe da CONTRATANTE;
- Analisar e mitigar riscos ao negócio;
- Estimar o impacto e janelas de indisponibilidade, se aplicável;
- Entregar a Arquitetura de Implementação para validação técnica da CONTRATANTE;
- Fornecer cronograma detalhado do projeto.

1.6.8.1.5. A CONTRATADA deverá configurar, instalar e testar os produtos, conforme projeto de implantação elaborado pela CONTRATADA e aprovado pela equipe técnica da CONTRATANTE, apresentando junto a cada produto o documento com instruções passo a passo para a sua instalação.

1.6.8.1.6. Os produtos fornecidos serão instalados e configurados em conformidade com o padrão da Rede da CONTRATANTE.

1.6.8.1.7. As ações de instalação, configuração e testes da solução serão realizadas pela CONTRATADA e deverão contemplar pelo menos as seguintes atividades:

- Análise preliminar da topologia e operação da Rede da CONTRATANTE com vistas a sua integração plena com a solução ofertada;
- Completa instalação e configuração, testes em produção e ajustes da solução ofertada;
- Implementação, com a coleta de evidências, dos controles de requisitos de segurança da CONTRATANTE, que forem possíveis de serem aplicados nos equipamentos/produtos da solução ofertada;
- Acompanhamento e homologação do ambiente de produção;

- Documentação detalhada de todos os passos da instalação, configuração e ajustes no ambiente de produção, a qual deverá ser entregue em arquivo eletrônico no formato PDF, antes da emissão do Termo de Recebimento Definitivo a ser expedido pela CONTRATANTE.

1.6.8.1.8. Os trabalhos serão coordenados e acompanhados pelos analistas e técnicos da CONTRATANTE, devendo haver repasse de conhecimento durante a execução dos serviços.

1.6.8.1.9. A critério da CONTRATANTE, os serviços poderão ser executados fora do horário comercial e/ou em finais de semana ou feriados sem custo adicional para a CONTRATANTE, visando minimizar os transtornos aos usuários pela eventual indisponibilidade da rede.

1.6.8.1.10. Para todos os efeitos, a conclusão dos serviços de instalação, configuração, testes em produção e ajustes será dada pela entrega da solução em pleno funcionamento, de acordo com as recomendações do(s) fabricante(s) e demais condições estabelecidas neste termo.

1.6.8.2. **Prazo de Execução**

1.6.8.2.1. O prazo total para a conclusão dos serviços de instalação, configuração, testes e documentação da solução não poderá ultrapassar 60 (sessenta) dias úteis, contados do início do serviço, salvo necessidade excepcional devidamente ajustada entre CONTRATANTE e CONTRATADA.

1.6.8.2.2. O responsável técnico pelo projeto deverá estar disponível e acessível durante toda a fase de implantação, que deverá contemplar, no mínimo, as seguintes etapas:

1.6.8.2.2.1. Planejamento: nesta etapa a CONTRATADA deverá realizar o planejamento do projeto, em que serão definidos os prazos por atividade, as pessoas, a estratégia de implantação do serviço, o plano de testes, bem como quaisquer outros itens necessários à implantação do projeto. Deverão considerar as janelas de manutenção da CONTRATANTE, plano de *rollback* e o escopo definido. Os responsáveis técnicos designados pela CONTRATANTE acompanharão e aprovarão o planejamento.

1.6.8.2.2.2. Cronograma: a CONTRATADA deverá, em conjunto com representantes da Superintendência de Tecnologia e Informação (STI), elaborar e apresentar o cronograma detalhado, contendo todas as fases e datas previstas para disponibilizar a solução para uso, inclusive treinamentos, observados os prazos estabelecidos neste termo.

1.6.8.2.2.3. Plano de Implementação: a CONTRATADA, antes de iniciar a execução das configurações, deverá elaborar documentação técnica denominada “Plano de Implementação” detalhando e fundamentando todas as configurações que serão realizadas.

1.6.8.2.2.4. Plano de Testes: a CONTRATADA deverá entregar documentação técnica denominada “Plano de Testes” de forma a garantir que todas as características exigidas neste termo tenham sido satisfeitas. Deverá incluir no mínimo:

- Teste das funcionalidades da solução;
- Teste de alta disponibilidade;
- Teste de qualidade;
- Teste de desempenho.

1.6.8.2.3. Desde que solicitado pela CONTRATANTE, a CONTRATADA deverá fornecer guia rápido de referência voltado aos usuários, customizado para utilização das

principais funcionalidades da solução.

1.6.8.2.4. Toda a documentação será analisada pela CONTRATANTE e deverá ser complementada pela CONTRATADA, caso seja solicitado.

1.6.8.2.5. Após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas e o cumprimento dos prazos pactuados.

1.6.8.2.6. A implantação deverá ocorrer conforme planejamento realizado e segundo as diretrizes da CONTRATANTE.

1.6.8.2.7. Finalização: a solução implantada será aceita, se e somente se, houver comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos. Essa comprovação será feita mediante observação direta das características dos componentes da solução, o funcionamento adequado das funções especificadas, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configuração.

1.6.8.2.8. Documentação Final: após a implementação, a CONTRATADA deverá entregar a documentação técnica final do projeto, contendo, no mínimo, a implementação realizada, arquitetura adotada, descrição e forma da redundância, instruções para *backup*/restauração, cópia das configurações realizadas em todos os elementos com comentários, número serial dos produtos entregues, lista de material dos produtos entregues. Deverá incluir outras informações que a CONTRATANTE ou a CONTRATADA julgarem importantes para o registro fiel de como a solução foi implementada. Essa documentação será denominada Documentação Final.

1.6.8.2.9. O Termo de Recebimento Definitivo da solução descrita no item 1 do lote 2 deste Termo de Referência será emitido e entregue à CONTRATADA após a finalização dos serviços de instalação, configuração e testes.

1.6.8.3. **Repasse de Conhecimento:**

1.6.8.3.1. Repasse de conhecimento da solução ofertada no item 1 do Lote 2, do tipo teórico e prático.

1.6.8.3.2. O(s) instrutor(es) deverá(ão) possuir conhecimento comprovado da solução fornecida.

1.6.8.3.3. Deverá ser realizado no ambiente da CONTRATANTE ou de forma on line, com aulas ao vivo e com material didático digital (PPT ou PDF, documentação do projeto e manuais de produto) fornecido pela CONTRATADA.

1.6.8.3.3.1. O repasse de conhecimento poderá ser gravado pela CONTRATANTE.

1.6.8.3.4. O repasse de conhecimento deverá ser realizado pela CONTRATADA para uma turma de 6 (seis) vagas, para analistas e técnicos da CONTRATANTE e deverá ser ministrado no turno matutino ou vespertino, conforme a necessidade da SEF/MG, em horário comercial e dias úteis.

1.6.8.3.5. O repasse de conhecimento compreenderá necessariamente os seguintes tópicos:

1.6.8.3.5.1. Instalação, configuração e operação do produto;

1.6.8.3.5.2. Apresentação do projeto da CONTRATANTE;

1.6.8.3.5.3. Descrição da arquitetura do produto;

1.6.8.3.5.4. Descrição dos *software* disponíveis no produto;

1.6.8.3.5.5. Estratégias de implementação do produto.

1.6.8.3.6. É responsabilidade da CONTRATANTE zelar pelo comparecimento e assiduidade dos servidores/analistas à capacitação aplicada.

1.6.8.3.7. A CONTRATANTE poderá solicitar a repetição do repasse de conhecimento caso entenda que o mesmo não cumpriu os requisitos estabelecidos.

1.6.8.3.8. O repasse de conhecimento não se confunde com o treinamento previsto para a solução.

1.6.9. **Lote 2 - Item 3 - Treinamento**

1.6.9.1. Treinamento completo da solução ofertada no item 1 Lote 2, do tipo teórico e prático.

1.6.9.2. Os instrutores deverão ser certificados pelo fabricante e possuir conhecimentos comprovados na solução fornecida.

1.6.9.3. A CONTRATADA deverá apresentar, quando da execução do contrato, certidão de capacidade técnica e documento comprobatório de parceria com o fabricante do produto e autorização para ministrar o treinamento oficial. Será aceito o fornecimento de treinamento oficial por meio da contratação de centro de treinamentos autorizado pelo fabricante.

1.6.9.4. A CONTRATADA disponibilizará laboratório que permita a simulação de ambientes com características similares aos propostos na solução implantada, possibilitando exercícios práticos de configuração do produto durante os módulos de capacitação em que tais atividades se apliquem. O ambiente de laboratório poderá ser montado em local disponibilizado pela CONTRATADA, em Belo Horizonte/MG, ou poderá estar nas dependências do fabricante e/ou fornecedor. Caso o laboratório esteja nas dependências do fabricante e/ou fornecedor, deverá ser acessado por meio de VPN/Internet, durante o período do treinamento, sendo de responsabilidade da CONTRATADA a disponibilização de local, em Belo Horizonte/MG, para realização do treinamento, bem como o acesso ao laboratório do fabricante e/ou fornecedor, com todos os recursos necessários (espaço físico, equipamentos, material didático, entre outros).

1.6.9.4.1. **Mediante formalização por parte da CONTRATADA, a CONTRATANTE poderá avaliar e aceitar que o treinamento seja feito de forma virtual. Nesse contexto, os técnicos a serem treinados deverão ter acesso à plataforma de treinamento do fornecedor ou do fabricante, mantendo-se as demais condições definidas nesta especificação**.

1.6.9.5. Em caso de treinamento presencial, o local deverá ser disponibilizado pela CONTRATADA na cidade de Belo Horizonte, devendo todos os custos (sala, instrutores, desktop, dentre outros) serem de responsabilidade da CONTRATADA.

1.6.9.6. Em caso de treinamento *on line*, as aulas deverão ser ao vivo e ministradas em língua portuguesa. Faculta-se à CONTRATANTE o direito de gravar as aulas.

1.6.9.7. O treinamento deverá ser realizado pela CONTRATADA, **em 1 (uma) turma de 6 (seis) vagas**, para analistas e técnicos da CONTRATANTE, perfazendo o total de horas/aula recomendado pelo fabricante da solução.

1.6.9.8. O treinamento estará centrado na solução fornecida, privilegiando atividades práticas que permitam melhor fixação do aprendizado, de forma a possibilitar à equipe técnica da CONTRATANTE gerenciar e administrar a solução implantada.

1.6.9.9. A CONTRATADA deverá fornecer, no início de cada tópico, apostilas (em formato impresso ou digital) que abordem todo o conteúdo programático, as quais poderão estar no todo ou em parte, em português e/ou inglês. O conteúdo do treinamento deverá abranger, pelo menos, os seguintes tópicos: instalação, configuração, operação, monitoramento, administração básica e avançada, relatórios.

1.6.9.10. O início dessa atividade, bem como o período e horário de realização, serão definidos pela CONTRATANTE em comum acordo com a CONTRATADA.

1.6.9.11. É responsabilidade da CONTRATANTE zelar pelo comparecimento e assiduidade dos treinandos à capacitação aplicada.

1.6.9.12. Ao final do treinamento deverá ser emitido certificado de conclusão para cada participante/aluno constando a carga horária e a ementa.

1.6.9.13. A CONTRATANTE poderá solicitar a repetição do treinamento caso entenda que o mesmo não cumpriu os requisitos estabelecidos.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

A proteção em camadas, também conhecida como defesa em profundidade, é uma estratégia de segurança que adota várias camadas de defesa para proteger recursos de informação. Trata-se de uma abordagem amplamente utilizada por organizações públicas e privadas ao redor do mundo visando à melhoria da postura de segurança. Para que seja continuamente aperfeiçoada, é importante a priorização dos investimentos definidos em conjunto pelas áreas da Superintendência de Tecnologia da Informação (STI). Se por um lado, a adoção da arquitetura em camadas traz consigo o desafio de integrar soluções de fabricantes distintos, por outro permite maior efetividade por parte dos times que trabalham diariamente para assegurar a confidencialidade, integridade e disponibilidade das informações e do ambiente da SEF/MG. Os benefícios da proteção em camadas são vários, com destaque para os seguintes:

- Diversidade de ameaças: existem diferentes tipos de ameaças à segurança da informação, incluindo *malware*, ataques de *phishing*, DDoS (negação de serviço), ransomware e violações de dados. Uma única solução de segurança não pode efetivamente se defender contra todas essas ameaças.
- Redundância: se uma camada de segurança falhar, outras estarão a postos para proteger os recursos de informação. Isso é especialmente importante quando se lida com ameaças avançadas que podem ser capazes de contornar certas defesas.
- Defesa contra ataques internos: nem todas as ameaças vêm de fora da organização. Às vezes, os funcionários podem acidentalmente causar uma violação de segurança, ou um ator mal-intencionado dentro da organização pode tentar acessar informações que não deveria. A proteção em camadas ajuda a defender contra esse tipo de ameaça.
- Visibilidade e controle: dispor de várias camadas de segurança fornece mais visibilidade sobre o que está acontecendo na rede e permite o controle mais granular sobre o tráfego.
- Cumprimento de regulamentos e boas práticas de mercado: regulamentos de segurança da informação, a exemplo da ISO 27001, adotada no âmbito da SEF/MG, além de boas práticas do mercado de segurança da informação, recomendam a adoção de defesa em profundidade.

Importante frisar que a segurança da informação é um processo contínuo e a proteção em camadas é apenas parte de uma estratégia de segurança eficaz. A secretaria concentra esforços no tripé: pessoas, processos e tecnologias. Por isso, é importante ter uma política de segurança sólida, oferecer treinamento regular aos funcionários, possuir planos de continuidade de negócios e de resposta a incidentes e realizar investimentos contínuos em soluções tecnológicas.

A crescente sofisticação das ameaças cibernéticas e a indispensabilidade da internet para as operações de negócios modernas tornam imperativo o investimento em plataformas robustas e abrangentes de segurança. A adoção de solução com funcionalidades como WAAP (Web Application and API Protection), proteção de DNS e SSE (Security Service Edge), não é apenas uma medida de precaução, mas um pilar estratégico para garantir a continuidade dos negócios, proteger ativos digitais e manter a confiança dos cidadãos e contribuintes.

Proteção Abrangente com Solução WAAP (WAF/Anti-DDoS e Certificados SSL/TLS)

A funcionalidade de WAAP (Web Application and API Protection), fornecida na modalidade Software as a Service (SaaS), é crucial para a defesa da linha de frente digital da SEF/MG. Ela abrange primordialmente:

- WAF (Web Application Firewall): Atua como escudo protetor para aplicações web e APIs, inspecionando o tráfego HTTP/S e bloqueando ameaças conhecidas e emergentes, como injeções de SQL (SQLi), cross-site scripting (XSS), inclusão de arquivos maliciosos e outras vulnerabilidades listadas no OWASP Top 10. Isso previne a exploração de falhas de segurança que poderiam levar a vazamentos de dados, interrupção de serviços ou comprometimento de sistemas.
- Anti-DDoS (Proteção contra Negação de Serviço Distribuída): Ataques DDoS visam sobrecarregar servidores e redes, tornando aplicações e serviços indisponíveis aos usuários legítimos. Uma solução

Anti-DDoS robusta é capaz de absorver e mitigar ataques volumétricos sofisticados, garantindo a continuidade das operações online e prevenindo perdas financeiras e danos à reputação associados à indisponibilidade. A franquia de 5TB de tráfego limpo ou throughput mensal equivalente assegura capacidade para lidar com grandes volumes de tráfego legítimo, mesmo sob ataque. Além disso, foi prevista franquia adicional, caso a quantidade original seja ultrapassada.

- Certificados SSL/TLS: A criptografia do tráfego entre o usuário e a aplicação web, proporcionada pelos certificados SSL/TLS, é fundamental para proteger dados sensíveis em trânsito (como credenciais de login, informações pessoais e dados fiscais). Além de garantir a privacidade e a integridade dos dados, o uso de SSL/TLS é um fator de ranqueamento em mecanismos de busca, essencial para construir a confiança do usuário, indicando que o site é seguro e autêntico.

Resiliência e Confiabilidade com Proteção de DNS

O DNS (Domain Name System) é um componente crítico da infraestrutura da internet, traduzindo nomes de domínio em endereços IP. No entanto, ele também é um vetor de ataque comum. Uma solução de DNS seguro protege contra uma variedade de ameaças, incluindo ataques DDoS direcionados aos servidores DNS, envenenamento de cache DNS (DNS cache poisoning) e falsificação de DNS (DNS spoofing). Ao garantir a disponibilidade e a integridade do serviço de DNS, a secretaria previnirá que usuários sejam redirecionados para sites maliciosos, que seus serviços fiquem inacessíveis ou que haja interceptação de tráfego, reforçando a segurança e a confiabilidade da presença online.

Otimização de Desempenho com CDN (Content Delivery Network)
As plataformas de segurança abrangentes integram funcionalidades de CDN (Content Delivery Network), que trazem benefícios significativos de desempenho e disponibilidade. Trata-se de uma rede de servidores distribuídos geograficamente que armazena cópias do conteúdo de um site (como imagens, vídeos, scripts) mais perto dos usuários finais. Dentre os principais benefícios do CDN destacam-se:

- Carregamento Mais Rápido: Ao entregar conteúdo a partir de um servidor mais próximo do usuário, o tempo de carregamento das páginas é drasticamente reduzido, melhorando a experiência do usuário.
- Redução de Latência: A proximidade dos servidores CDN diminui a latência, ou seja, o tempo que os dados levam para viajar entre o servidor e o usuário.
- Maior Escalabilidade e Disponibilidade: A CDN distribui o tráfego entre múltiplos servidores, aumentando a capacidade de lidar com picos de acesso, melhorando a resiliência contra falhas no servidor de origem. Isso também complementa a proteção Anti-DDoS ao absorver grandes volumes de tráfego.
- Menor Consumo de Banda da Origem: Como parte do conteúdo é entregue pela CDN, o servidor de origem experimenta carga menor e, consequentemente, menor consumo de banda, o que pode levar à redução de custos de hospedagem.

Segurança Moderna e Acesso Seguro com Solução SSE (Security Service Edge)

A SSE (Security Service Edge) é uma arquitetura de segurança moderna que converge diversas funcionalidades de rede e segurança na nuvem, sendo essencial para organizações com força de trabalho distribuída, usuários remotos e adoção crescente de aplicações em nuvem.

O SSE oferece um conjunto de serviços de segurança, como ZTNA (Zero Trust Network Access), SWG (Secure Web Gateway) e CASB (Cloud Access Security Broker). Essa abordagem permite aplicar políticas de segurança consistentes e granulares, independentemente da localização do usuário ou do dispositivo, protegendo contra ameaças da web, controlando o acesso a aplicações SaaS e garantindo que apenas usuários autorizados acessem recursos específicos com base no princípio de "menor privilégio". Ao consolidar múltiplas funções de segurança em uma única plataforma entregue na nuvem, o SSE reduz a complexidade da infraestrutura de segurança, simplifica o gerenciamento, diminuindo os custos operacionais. Ele também melhora a experiência do usuário, fornecendo acesso seguro e rápido a aplicações e dados, de qualquer lugar.

Benefícios Estratégicos da Contratação

A contratação das soluções previstas no Termo de Referência com as funcionalidades descritas proporcionará:

- Minimização da probabilidade e do impacto de incidentes de segurança, como vazamentos de dados, interrupções de serviço e ataques de ransomware.
- Garantia da disponibilidade de aplicações e serviços críticos, mesmo diante de ataques sofisticados.
- Manutenção da confiança de cidadãos e contribuintes ao demonstrar compromisso com a segurança da informação.
- Entrega de conteúdo mais rápida e confiável, resultando em melhor experiência para os usuários dos serviços.
- Auxílio no cumprimento de diversas regulamentações e padrões de segurança de dados.
- Potencial redução de custos associados a incidentes de segurança.

Investir em uma Plataforma de Acesso Seguro à Internet com as funcionalidades de WAAP (incluindo WAF/Anti-DDoS e SSL/TLS), CDN, Proteção de DNS e SSE é uma decisão estratégica fundamental para proteger os ativos digitais da SEF/MG, assegurar a continuidade operacional, otimizar o desempenho das aplicações web e habilitar o crescimento seguro no ambiente digital cada vez mais complexo e hostil. Trata-se de uma medida proativa que fortalece a postura de segurança e a performance digital da secretaria, preparando-a para os desafios presentes e futuros.

Pelos motivos expostos, recomenda-se fortemente o investimento nas soluções propostas , permitindo que a Secretaria de Estado de Fazenda de Minas Gerais (SEF/MG) mitigue os impactos negativos dos incidentes, fortalecendo a segurança da informação e garantindo o cumprimento das normas, refletindo o compromisso contínuo com a proteção dos ativos de informação do órgão.

3. REQUISITOS DA CONTRATAÇÃO

3.1. **Da Participação de Consórcios:**

3.1.1. Não será permitida a participação de empresas reunidas em consórcio.

3.2. **Da Participação de Cooperativa**:

3.2.1. Não será permitida a participação de sociedades cooperativas.

3.3. **Da Subcontratação:**

3.3.1. É vedada a subcontratação total ou das parcelas tecnicamente mais complexas ou de valor mais significativo do objeto, que motivaram a comprovação de capacidade financeira ou técnica.

3.3.2. É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau, conforme art. 122, §3º, da Lei Federal n° 14.133, de 2021.

3.4. **Da Sustentabilidade**:

3.4.1. Não há viabilidade de adoção de critérios ou práticas de sustentabilidade na presente contratação.

3.5. **Da Indicação de Marcas ou Modelos:**

3.5.1. Não serão exigidas marcas ou modelos específicos para a contratação.

3.6. **Da Vedação de Utilização de Marca ou Modelo**:

3.6.1. Não haverá vedação de marca/modelo na presente contratação.

3.7. **Da Exigência de Carta de Solidariedade**:

3.7.1. Não será exigida a apresentação de carta de solidariedade na presente contratação.

3.8. **Da Garantia da Contratação**:

3.8.1. Será exigida a garantia de execução da contratação, nos moldes do art. 96 e seguintes da Lei Federal nº 14.133, de 2021, no percentual de 5% do valor total inicial do contrato, conforme regras a serem estabelecidas na minuta contratual.

3.8.2. A garantia será posterior à assinatura do contrato, devendo ser prestada em até 15 (quinze) dias corridos.

3.9. **Condições e Especificações da Garantia do Serviço:**

3.9.1. Será aplicada ao serviço somente a garantia legal estabelecida pelo art. 26, da Lei Federal nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor – CDC).

3.10. **Da Vistoria**:

3.10.1. Não há necessidade de realização de vistoria prévia ao local de execução dos serviços.

4. MODELO DE EXECUÇÃO DO OBJETO

4.1. **Do Prazo e das Condições da Prestação do Serviço**:

4.1.1. A execução do objeto seguirá a seguinte dinâmica:

4.1.1.1. **Lote 1 - Itens 1 e 3**: até 30 (trinta) dias úteis, contados a partir da emissão da Nota de Empenho, de acordo com os módulos a serem habilitados a critério da CONTRATANTE.

4.1.1.2. **Lote 1 - Item 4:** início em até 15 (quinze) dias úteis, contados do Recebimento Provisório dos itens 1 e 3 e término em até 60 (sessenta) dias úteis após o início dos serviços de instalação, salvo situação excepcional devidamente ajustada entre CONTRATANTE e CONTRATADA.

4.1.1.3. **Lote 1 - Item 5**: até 120 (cento e vinte) dias úteis, contados da expedição do Termo de Recebimento Definitivo para os itens 1 e 3.

4.1.1.4. **Lote 2 - Item 1**: até 30 (trinta) dias úteis, contados a partir da emissão da Nota de Empenho, de acordo com os módulos a serem habilitados a critério da CONTRATANTE.

4.1.1.5. **Lote 2 - Item 2:** início em até 15 (quinze) dias úteis, contados do Recebimento Provisório do item 1 e término em até 60 (sessenta) dias úteis após o início dos serviços de instalação, salvo situação excepcional devidamente ajustada entre CONTRATANTE e CONTRATADA.

4.1.1.6. **Lote 2 - Item 3**: até 120 (cento e vinte) dias úteis, contados da expedição do Termo de Recebimento Definitivo para o item 1.

4.2. **Do Local e Horário da Prestação do Serviço:**

4.2.1. Os serviços deverão ser prestados no seguinte endereço: Superintendência de Tecnologia da Informação da Secretaria de Estado de Fazenda de Minas Gerais, localizada à Rua da Bahia, nº 1816, 1º e 2º subsolos, bairro de Lourdes, em Belo Horizonte [inserir endereço], no horário a ser determinado pela CONTRATANTE em acordo com a CONTRATADA [inserir horário].

4.2.2. Os serviços serão prestados remotamente e, caso seja necessário, no seguinte endereço: Superintendência de Tecnologia da Informação da Secretaria de Estado de Fazenda de Minas Gerais, localizada à Rua da Bahia, nº 1816, 1º e 2º subsolos, bairro de Lourdes, em Belo Horizonte, no horário a ser determinado pela CONTRATANTE em acordo com a CONTRATADA.

4.3. **Dos Materiais a Serem Disponibilizados**:

4.3.1. Não será necessário disponibilizar materiais de consumo e de uso duradouro.

4.4. **Do Regime de Execução**:

4.4.1. O regime de execução do contrato será [INSERIR O REGIME DE EXECUÇÃO ESCOLHIDO].

5. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

5.1. **Do Recebimento**:

5.1.1. Os serviços prestados serão recebidos provisoriamente pelo(a) responsável pelo acompanhamento e fiscalização do contrato, mediante termo(s) detalhado(s), quando verificado o cumprimento das exigências de caráter técnico e administrativo.

5.1.1.1. Salvo disposição em contrário no contrato, em ato normativo ou neste Termo de Referência, os ensaios, os testes e as demais provas para aferição da boa execução do objeto do contrato exigidos por normas técnicas oficiais correrão por conta da CONTRATADA.

5.1.2. Para efeito de recebimento provisório, ao final de cada período de faturamento, o responsável pelo acompanhamento e fiscalização do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à CONTRATADA, registrando em relatório a ser encaminhado ao gestor do contrato.

5.1.3. A CONTRATADA fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

5.1.4. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

5.1.5. Os serviços prestados serão recebidos definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo(s) detalhado(s) que comprove(m) o atendimento das exigências contratuais, no prazo de até [inserir número de dias] ([escrever por extenso]) dias corridos, contados a partir do recebimento provisório.

5.1.6. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

5.1.7. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

5.1.8. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei Federal nº 14.133, de 2021, notificando o Contratado para emissão de nota fiscal no que diz respeito à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

5.1.9. O prazo para a solução pelo CONTRATADO de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

5.1.10. O recebimento provisório ou definitivo não exclui a responsabilidade civil do CONTRATADO pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

5.2. **Da Avaliação da Execução do Objeto:**

5.2.1. A avaliação da execução do objeto utilizará [o Instrumento de Medição de

Resultado (IMR), conforme previsto no [Anexo [.....] **OU** documento que o substitua].

5.2.2. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para avaliação da prestação dos serviços.

5.2.3. [Inserir demais critérios de medição, conforme o objeto a ser contratado, quando cabível].

5.3. **Da Liquidação**:

5.3.1. A Liquidação será efetuada no prazo de até [inserir número de dias] ([escrever por extenso]) dias corridos contados da data do recebimento definitivo do serviço e respectivo aceite do Contratante.

5.3.2. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

5.3.2.1. O vencimento;

5.3.2.2. A data da emissão;

5.3.2.3. Os dados do contrato e do órgão Contratante;

5.3.2.4. O período respectivo de execução do objeto;

5.3.2.5. O valor a pagar; e

5.3.2.6. Eventual destaque do valor de retenções tributárias cabíveis.

5.3.3. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante.

5.3.4. A nota fiscal, ou o instrumento de cobrança equivalente, deverá ser acompanhada da comprovação da regularidade fiscal disposta no art. 68 da Lei Federal nº 14.133, de 2021.

5.4. **Do Pagamento**:

5.4.1. O pagamento será efetuado através do Sistema Integrado de Administração Financeira - SIAFI/MG, por meio de ordem bancária emitida por processamento eletrônico, a crédito do beneficiário em um dos bancos que o Contratado indicar, no prazo de até [inserir número de dias] ([escrever por extenso]) dias corridos, contados a partir da data final da liquidação a que se referir, com base nos documentos fiscais devidamente conferidos e aprovados pelo Contratante.

5.4.1.1. A Administração deve observar a ordem cronológica nos pagamentos, conforme disposto no art. 141 da Lei Federal nº 14.133, de 2021.

5.4.2. No caso de atraso pelo CONTRATANTE, por culpa exclusiva da Administração, os valores devidos ao CONTRATADO serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, de acordo com a variação do [indicar o índice ou taxa que deverá ser utilizado].

5.4.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

5.4.3.1. Independentemente do percentual de tributo inserido pelo CONTRATADO na planilha de custo, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

5.4.4. O CONTRATADO deve garantir a manutenção dos requisitos de habilitação previstos neste documento durante toda a contratação.

5.4.4.1. Eventuais situações de irregularidades fiscal ou trabalhista do CONTRATADO não impedem o pagamento, se o objeto tiver sido executado e atestado. Tal hipótese ensejará, entretanto, a adoção das providências tendentes ao sancionamento

do CONTRATADO e rescisão contratual.

5.4.5. O CONTRATADO regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

5.4.6. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que o CONTRATADO:

5.4.6.1. Não produziu os resultados acordados;

5.4.6.2. Deixou de executar, ou não executou com a qualidade mínima exigida as atividades contratadas; ou

5.4.6.3. Deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

5.5. **Da Antecipação do Pagamento:**

5.5.1. A presente contratação permite a antecipação de pagamento [parcial **OU** total].

5.5.2. O Contratado emitirá [recibo **OU** nota fiscal **OU** fatura **OU** documento idôneo] correspondente ao valor da antecipação de pagamento de R$ [inserir o valor] ([inserir valor por extenso]), tão logo [incluir condicionante – ex: seja assinado o termo de contrato, ou seja, prestada a garantia etc.], para que o Contratante efetue o pagamento antecipado.

5.5.3. Para as etapas seguintes do contrato, a antecipação do pagamento ocorrerá da seguinte forma:

5.5.3.1. R$ [inserir valor] ([inserir valor por extenso]) quando do início da segunda etapa.

5.5.3.2. (...)

5.5.4. Fica o Contratado obrigado a devolver, com correção monetária, a integralidade do valor antecipado na hipótese de inexecução do objeto.

5.5.4.1. No caso de inexecução parcial, deverá haver a devolução do valor relativo à parcela não-executada do contrato.

5.5.4.2. O valor relativo à parcela antecipada e não executada do contrato será atualizado monetariamente pela variação acumulada do ..... (especificar o índice de correção monetária a ser adotado), ou outro índice que venha a substituí-lo, desde a data do pagamento da antecipação até a data da devolução.

5.5.5. A liquidação ocorrerá de acordo com as regras do tópico respectivo deste instrumento.

5.5.6. O pagamento antecipado será efetuado no prazo máximo de até [inserir prazo] ([inserir prazo por extenso]) dias, contados do recebimento do ..... (recibo **OU** nota fiscal **O U** fatura **OU** documento idôneo).

5.5.7. A antecipação de pagamento dispensa o ateste ou recebimento prévios do objeto, os quais deverão ocorrer após a regular execução da parcela contratual a que se refere o valor antecipado.

5.5.8. O pagamento de que trata este item está condicionado à tomada das seguintes providências pelo Contratado:

5.5.8.1. comprovação da execução da etapa imediatamente anterior do objeto pelo Contratado, para a antecipação do valor remanescente;

5.5.8.2. prestação da garantia adicional nas modalidades de que trata o art. 96 da Lei Federal nº 14.133, de 2021, no percentual de [inserir percentual]% ([inserir percentual por extenso]).

5.5.9. O pagamento do valor a ser antecipado ocorrerá respeitando eventuais retenções tributárias incidentes.

6. PROCEDIMENTO DE TRANSIÇÃO E FINALIZAÇÃO DO CONTRATO

6.1. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

7. MODELO DE GESTÃO DA CONTRATAÇÃO

7.1. **Regras Gerais**:

7.1.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as disposições da Lei Federal nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial, conforme art. 115 da referida Lei, e artigos 15 e 16 do Decreto nº 48.587, de 17 de março de 2023.

7.1.2. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.1.3. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

7.1.4. Após a assinatura do contrato ou retirada/aceitabilidade de instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial visando a apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução do Contratado, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

7.1.5. A execução do contrato deverá ser acompanhada e fiscalizada por 1 (um) ou mais gestores e fiscais do contrato, representantes da Administração especialmente designados conforme requisitos estabelecidos no art. 7º da Lei Federal nº 14.133, de 2021, ou pelos respectivos substitutos, conforme art. 117 da Lei Federal nº 14.133, de 2021, e art. 14 do Decreto nº 48.587, de 2023.

7.1.6. Constatada a ocorrência de descumprimento total ou parcial do contrato, deverão ser observadas as disposições dos art. 155 a 163 da Lei Federal nº 14.133, de 2021, a fim de apurar a responsabilidade do Contratado e eventualmente aplicar sanções.

7.2. **Da Fiscalização do Contrato**:

7.2.1. O fiscal do contrato prestará apoio técnico e operacional ao gestor do contrato com informações pertinentes às suas competências, nos termos do inciso I do art. 16 do Decreto nº 48.587, de 2023.

7.2.2. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados, de acordo com o § 1º, art. 117 da Lei Federal nº 14.133, de 2021, e nos termos do inciso II do art. 16 do Decreto nº 48.587, de 2023.

7.2.3. O fiscal do contrato emitirá notificações para a correção de rotinas ou de qualquer inexatidão ou irregularidade constatada, com a definição de prazo para a correção, nos termos do inciso III do art. 16 do Decreto nº 48.587, de 2023.

7.2.4. O fiscal do contrato informará a seus superiores e ao gestor do contrato, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência, conforme § 2º, art. 117 da Lei Federal nº 14.133, de 2021, e inciso IV do art. 16 do Decreto nº 48.587, de 2023.

7.2.5. O fiscal do contrato comunicará imediatamente ao gestor do contrato quaisquer ocorrências que possam inviabilizar a execução do contrato nas datas estabelecidas, nos termos do inciso V, do art. 16 do Decreto nº 48.587, de 2023.

7.2.6. O fiscal do contrato fiscalizará a execução do contrato para que sejam cumpridas as condições estabelecidas, de modo a assegurar os melhores resultados para a Administração, com a conferência das notas fiscais e das documentações exigidas para o pagamento e, após o

ateste, que certifica o recebimento provisório, encaminhar ao gestor de contrato, nos termos do inciso VI, do art. 16 do Decreto nº 48.587, de 2023.

7.2.7. O fiscal do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual, nos termos do inciso VII, do art. 16 do Decreto nº 48.587, de 2023.

7.2.8. O fiscal do contrato realizará o recebimento provisório do objeto do contrato, mediante termo detalhado que comprove o cumprimento das exigências contratuais, nos termos do inciso VIII, do art. 16 do Decreto nº 48.587, de 2023.

7.2.9. A fiscalização de que trata esta cláusula não exclui, nem reduz a responsabilidade do Contratado por quaisquer irregularidades, inexecuções ou desconformidades havidas na execução do objeto, aí incluídas imperfeições de natureza técnica ou aquelas provenientes de vício redibitório, como tal definido pela lei civil.

7.2.10. Os seguintes servidores serão os designados pela autoridade competente para acompanhar e fiscalizar o contrato, como representantes da Administração:

7.2.10.1. Daniel de Oliveira Rezende - Masp 669.570-4 (titular);

7.2.10.2. Luciano Marques Viana - Masp Masp. 669.700-7 (suplente).

7.3. **Da Gestão do Contrato:**

7.3.1. O gestor do contrato orientará os fiscais de contrato no desempenho de suas atribuições, nos termos do inciso I, do art. 15 do Decreto nº 48.587, de 2023.

7.3.2. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato ou terceiros contratados, das ocorrências relacionadas à execução do contrato e as medidas adotadas, e informará à autoridade superior àquelas que ultrapassarem a sua competência, nos termos do inciso II, do art. 15 do Decreto nº 48.587, de 2023.

7.3.3. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e de pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais, nos termos do inciso III, do art. 15 do Decreto nº 48.587, de 2023.

7.3.4. O gestor do contrato coordenará a autuação da rotina de acompanhamento e de fiscalização do contrato, cujo histórico de gerenciamento deverá conter todos os registros formais da execução, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, nos termos do inciso IV, do art. 15 do Decreto nº 48.587, de 2023.

7.3.5. O gestor do contrato coordenará os atos preparatórios relativos à instrução processual e ao envio da documentação pertinente ao setor de contratos para formalização da celebração de aditivos, prorrogações, reajustes ou rescisões contratuais, nos termos do inciso V, do art. 15 do Decreto nº 48.587, de 2023.

7.3.6. O gestor do contrato realizará o recebimento definitivo do objeto do contrato, mediante termo detalhado que comprove o atendimento das exigências contratuais, nos termos do inciso VI, do art. 15 do Decreto nº 48.587, de 2023.

7.3.7. O gestor do contrato elaborará o relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração, de que trata a alínea "d" do inciso VI do § 3º do art. 174 da Lei Federal nº 14.133, de 2021, nos termos do inciso VII, do art. 15 do Decreto nº 48.587, de 2023.

7.3.8. O gestor do contrato tomará as providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei Federal nº 14.133, de 2021, ou pelo agente ou pelo setor competente para tal, conforme o caso, nos termos do inciso VIII, do art. 15 do Decreto nº 48.587, de 2023.

7.3.9. Os seguinte servidores serão os designados pela autoridade competente para fazer a gestão do contrato, como representantes da Administração:

7.3.9.1. Alessandro Márcio M. Zebral - Masp: 340.218-7 (titular);

7.3.9.2. Fabiana Inácia da Silva - Masp: 669.005-1 (suplente).

7.4. **Do Preposto:**

7.4.1. Não será necessária a designação de preposto pelo Contratado.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

8.1. O fornecedor será selecionado por meio da realização de procedimento na modalidade pregão, conforme art. 28 da Lei Federal nº 14.133, de 2021, sob a forma eletrônica, com adoção do critério de julgamento pelo menor preço, conforme art. 33, da referida Lei Federal.

8.1.1. O fornecedor somente poderá oferecer lance de valor inferior em relação ao último lance por ele ofertado, observado o intervalo mínimo de diferença de valores entre os lances.

8.1.2. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao que cobrir a melhor oferta é de R$10.000,00 (dez mil reais).

8.2. **Dos Critérios da Aceitabilidade da Proposta**:

8.2.1. A proposta terá validade de 90 (noventa) dias corridos contados da data de sua apresentação.

8.3. **Da Prova de Conceito (PoC):**

8.3.1. Será exigida prova de conceito, conforme disposto no §3º, art. 17 e inciso II, art. 41 da Lei Federal nº 14.133, de 2021, para comprovação de que os serviços prestados possuem funcionalidade de acordo com as especificações técnicas solicitadas neste Termo de Referência.

8.3.2. Concluída a etapa de lances do pregão, o licitante classificado provisoriamente em primeiro lugar, deverá apresentar a utilização e o funcionamento da solução, no prazo de até 5 (cinco) dias úteis. Nesse momento, a CONTRATANTE dará início à fase de Prova de Conceito da solução proposta.

8.3.3. A Prova de Conceito compreende:

8.3.3.1. A data da realização da Prova de Conceito deverá ser informada pela Pregoeira na própria sessão pública a todos os licitantes participantes.

8.3.3.2. Nessa reunião:

8.3.3.2.1. O licitante deverá fornecer todos os requisitos para realização da prova de Conceito e ceder todos os acessos necessários e suficientes aos técnicos da SEF/MG para a verificação de no mínimo, os requisitos exigidos no Anexo I (113522336), para que a solução apresentada pelo licitante possa ser avaliada.

8.3.3.2.2. A Prova de Conceito acontecerá no ambiente padrão de teste do fabricante da solução.

8.3.4. Disponibilização: o licitante deverá apresentar a utilização e o funcionamento da solução, no prazo máximo de 5 (cinco) dias úteis, contados a partir da data de suspensão da sessão pública do Pregão, em horário comercial (das 9h às 18h). O licitante deverá disponibilizar 1 (um) técnico que se responsabilizará pela disponibilização e configuração dos software da solução.

8.3.5. O licitante deverá apresentar a documentação técnica da solução integrada, contemplando informações detalhadas de todos os itens e modelos que compõem a mesma, conforme descrito neste termo.

8.3.6. O ambiente deverá estar preparado para permitir a execução de qualquer uma das funcionalidades listadas na especificação de requisitos, definidas a critério da

CONTRATANTE constantes deste termo.

8.3.7. Não caberá a CONTRATANTE prover o ambiente necessário (equipamentos e infraestrutura) para o acesso à solução integrada, cabendo ao licitante a comprovação do atendimento dos requisitos constantes neste termo. O provimento do ambiente utilizado exclusivamente para os testes da etapa de prova de conceito inclui o fornecimento de toda a infraestrutura necessária. A composição do ambiente necessário será de total responsabilidade do licitante.

8.3.8. Comprovação: esta etapa será realizada por um período máximo de 2 (dois) dias úteis, a contar do dia seguinte à conclusão do prazo para a etapa de disponibilização, conforme informado pelo pregoeiro em sessão pública. A partir do primeiro dia dessa etapa, o licitante deverá:

8.3.8.1. Disponibilizar 1 (um) técnico que se responsabilizará pela comprovação das funcionalidades e requisitos descritos neste termo, por meio de testes práticos ou por comandos de configuração. A aprovação das funcionalidades existentes na solução, apresentada pelo licitante será efetuado pela equipe técnica da SEF/MG.

8.3.8.2. A entrega da documentação devidamente preenchida não exclui a necessidade de comprovação do atendimento aos requisitos por meio de testes práticos ou por comandos de configuração durante a realização da Prova de Conceito.

8.3.9. Local e Horário da Prova de Conceito: a data da realização da Prova de Conceito e respectivos horários deverão ser informados pela pregoeira na sessão pública do pregão para todos os licitantes participantes do Pregão.

8.3.10. É facultado a cada participante indicar um representante técnico para acompanhamento das verificações de conformidade, em data a ser divulgada durante a sessão pública.

8.3.11. O licitante que abandonar a execução da Prova de Conceito, ou deixar de enviar a documentação exigida nesta seção/título, bem como descumprir os prazos e regras estabelecidos, será desclassificado, sem prejuízo das sanções cabíveis.

8.3.12. A não comprovação dos requisitos exigidos na Prova de Conceito importará a desclassificação do licitante classificado provisoriamente no certame, quando o pregoeiro convocará o próximo licitante detentor de proposta válida, obedecida a classificação na etapa de lances, sucessivamente, até que um licitante cumpra os requisitos previstos neste Termo de Referência e seja declarado vencedor.

8.3.13. Os resultados das avaliações serão divulgados no chat, no dia e horário da reabertura da sessão pública do Pregão, previamente informados pela Pregoeira.

9. HABILITAÇÃO

9.1. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

9.1.1. **Habilitação Jurídica**:

9.1.1.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

9.1.1.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

9.1.1.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

9.1.1.4. Sociedade empresária, Sociedade Limitada Unipessoal – SLU ou sociedade identificada como Empresa Individual de Responsabilidade Limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

9.1.1.5. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

9.1.1.6. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

9.1.1.7. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

9.1.1.8. ~~Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971;~~

9.1.1.9. ~~Agricultor familiar: Declaração de Aptidão ao Programa Nacional de Fortalecimento à Agricultura Familiar – PRONAF-DAP, nos termos do art. 16 do Decreto nº 46.712, de 29 de janeiro de 2015;~~

9.1.1.10. ~~Produtor Rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB nº 971, de 13 de novembro de 2009 (arts. 17 a 19 e 165);~~

9.1.1.11. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

9.1.2. **Habilitação Fiscal, Social e Trabalhista**:

9.1.2.1. Inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ).

9.1.2.2. Inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual.

9.1.2.3. Regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede do fornecedor, ou outra equivalente, na forma da lei.

I - A prova de regularidade fiscal e seguridade social perante a Fazenda Nacional será efetuada mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil – RFB e pela Procuradoria-Geral da Fazenda Nacional – PGFN, referente a todos os tributos federais e à Dívida Ativa da União – DAU por elas administrados, bem como das contribuições previdenciárias e de terceiros.

II - Caso o fornecedor seja considerado isento dos tributos estaduais e/ou municipais referentes ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

9.1.2.4. Certificado de Regularidade relativa à seguridade social e perante o Fundo de Garantia por Tempo de Serviço – FGTS.

9.1.2.5. Prova de inexistência de débitos inadimplidos perantea Justiça do Trabalho, mediante a apresentação de certidão negativa, ou positiva com efeito de negativa, nos termos da Lei Federal nº 12.440, de 7 de julho de 2011, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943.

9.1.2.6. Comprovação da regularidade fiscal e/ou trabalhista deverá ser efetuada mediante a apresentação das competentes certidões negativas de débitos, ou positivas com efeitos de negativas.

9.1.3. **Qualificação Econômico-Financeira**:

9.1.3.1. Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do fornecedor, emitida nos últimos 06 (seis) meses.

9.1.4. **Qualificação técnico-operacional e técnico-profissional**:

9.1.4.1. Não será exigida a apresentação de documentos relativos à qualificação técnico-operacional e técnico-profissional.

OU

9.1.4.1. Declaração de que o fornecedor tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto desta contratação.

I - A declaração acima poderá ser substituída por declaração formal assinada pelo responsável técnico do interessado acerca do conhecimento pleno das condições e peculiaridades da contratação.

9.1.4.2. Registro ou inscrição da empresa na entidade profissional .....(escrever por extenso, se o caso), em plena validade;

9.1.4.3. Para o(s) lote(s) / item(ens) [inserir o número do lote/item] deverá ser apresentada comprovação de aptidão para a prestação de serviços similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido (s) pelo conselho profissional competente, quando for o caso, bem como documentos comprobatórios emitidos na forma do § 3º do art. 88 da Lei Federal nº 14.133, de 2021, atendendo ao quantitativo mínimo de [inserir percentual]% ([inserir percentual por extenso] por cento) das quantidades apresentadas no subitem 1.1 do Termo de Referência, conforme §§ 2º e 5º do art. 67 da Lei Federal nº 14.133, de 2021.

I - Para atendimento do quantitativo indicado acima, é admitido o somatório de diferentes atestados, podendo ser de períodos concomitantes, desde que compatíveis com as características do objeto da licitação.

II - Os atestados deverão conter:

a) Nome empresarial e dados de identificação da instituição emitente (CNPJ, endereço, contato);

b) Local e data de emissão;

c) Nome, cargo, contato e a assinatura do responsável pela veracidade das informações;

d) Período da execução da atividade e quantitativo do objeto fornecido.

III - Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

IV - O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do Contratante e local em que foi executado o objeto contratado, dentre outros documentos.

9.1.4.4. Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

9.1.4.5. Em caso de apresentação de atestado de desempenho anterior emitido em favor de consórcio do qual o fornecedor tenha feito parte, se o atestado ou o contrato de constituição do consórcio não identificar a atividade desempenhada por cada consorciado individualmente, serão adotados os seguintes critérios na avaliação de sua qualificação técnica:

I - Caso o atestado tenha sido emitido em favor de consórcio homogêneo, cujas empresas possuem objeto social similar, as experiências atestadas deverão ser reconhecidas para cada empresa consorciada na proporção quantitativa de sua participação no consórcio;

II - Caso o atestado tenha sido emitido em favor de consórcio heterogêneo, cujas empresas possuem objeto social diverso, as experiências atestadas deverão ser reconhecidas para cada consorciado de acordo com os respectivos campos de atuação;

III - Na hipótese do item 9.1.4.5, para fins de comprovação do percentual de participação do consorciado, caso este não conste expressamente do atestado ou da certidão, deverá ser juntada ao atestado ou à certidão cópia do instrumento de constituição do consórcio.

9.1.4.6. [Inserir outra qualificação técnico-operacional e/ou técnico profissional conforme especificidades do objeto, limitada àquelas dispostas no art. 67 da Lei Federal nº 14.133, de 2021, mediante justificativa].

9.1.5. **Declaração**:

9.1.5.1. Declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei nos termos do art. 93 da Lei Federal nº 8.213, de 1991 e em outras normas específicas, conforme previsto no inciso IV do art. 63 da Lei Federal nº. 14.133, de 2021.

9.1.5.2. Caso o licitante não cumpra os requisitos exigidos em sede de declaração, deverá apresentar justificativa e documentos comprobatórios dos fatos alegados, para fins de análise da Administração.

9.1.6. **Habilitação de Consórcios**:

9.1.6.1. No caso da participação de empresas reunidas em consórcio, deverá acompanhar os documentos de habilitação, a comprovação de compromisso público ou particular do consórcio, subscrito pelas empresas consorciadas, com apresentação da proporção de participação de cada uma das consorciadas e indicação da empresa líder, que deverá representar as consorciadas perante o Estado de Minas Gerais, observadas as normas do art. 15 da Lei Federal nº 14.133, de 2021.

9.1.6.2. Deverão ser apresentados os documentos previstos no item referente à Habilitação, por parte de cada consorciado, admitindo-se, para efeito de qualificação técnica, o somatório dos quantitativos de cada consorciado, e, para efeito de qualificação econômico-financeira, o somatório dos valores de cada consorciado, na proporção de sua respectiva participação.

9.1.6.3. As empresas consorciadas serão solidariamente responsáveis pelas obrigações do consórcio na fase de licitação e durante a execução do contrato.

9.1.6.4. Antes da celebração do contrato, deverá ser promovida a constituição e o registro do consórcio, nos termos do compromisso referido no item 9.1.6.1.

9.1.6.5. Apenas os consórcios compostos exclusivamente por beneficiários indicados no caput do art. 3º do Decreto 47.437, de 2018 poderão usufruir dos benefícios legais da Lei Complementar Federal nº 123, de 2006, desde que a soma do faturamento das empresas consorciadas não ultrapasse o limite previsto no inciso II, artigo 3º, da Lei Complementar Federal nº 123, de 2006.

9.1.6.6. Não é permitido que uma empresa, consorciada simultaneamente em mais de um consórcio ou de forma isolada, participe do mesmo procedimento de contratação.

9.1.6.7. A substituição de consorciado deverá ser expressamente autorizada pelo órgão ou entidade contratante e condicionada à comprovação de que a nova empresa do consórcio possui, no mínimo, os mesmos quantitativos para efeito de habilitação técnica e os mesmos valores para efeito de qualificação econômico-financeira apresentados pela empresa substituída para fins de habilitação do consórcio no procedimento que originou o contrato.

9.1.7. **Habilitação de Cooperativas**:

9.1.7.1. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

I - A relação dos cooperados que atendem aos requisitos técnicos exigidos para a

contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§ 2º a 6º da Lei n. 5.764, de 1971;

II - A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

III - A comprovação do capital social proporcional ao número de cooperados necessários à execução contratual;

IV - O registro previsto na Lei n. 5.764, de 1971, art. 107;

V - A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato;

VI - A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador;

VII - Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: i) ata de fundação; ii) estatuto social com a ata da assembleia que o aprovou; iii) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; iv) editais de convocação das três últimas assembleias gerais extraordinárias; v) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e vi) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da contratação.

10. OBRIGAÇÕES ESPECÍFICAS DAS PARTES

10.1. Do Contratante:

10.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o presente Termo de Referência, o contrato ou documento que o substitua e seus anexos.

10.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência.

10.1.3. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto prestado, para que seja por ele reparado, corrigido, removido, reconstruído ou substituído, no total ou em parte, às suas expensas.

10.1.4. Acompanhar e fiscalizar a execução do contrato, atestar nas notas fiscais/faturas da efetiva prestação do serviço, objeto deste Termo de Referência.

10.1.5. Rejeitar, no todo ou em parte os serviços prestados, quando em desacordo com as especificações constantes na nota de empenho, no Termo de Referência e/ou na proposta comercial do Contratado.

10.1.6. Comunicar o Contratado para emissão de nota fiscal pertinente à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia parcial sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei Federal nº 14.133, de 2021.

10.1.7. Solicitar o reparo, a correção, a remoção ou a substituição do objeto em que se verificarem vícios, defeitos ou incorreções.

10.1.8. Efetuar o pagamento ao Contratado do valor correspondente à parcela do serviço prestado, no prazo, forma e condições estabelecidos no presente Termo de Referência.

10.1.9. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo Contratado durante a execução do contrato ou documento que o substitua.

10.1.10. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

10.1.10.1. A Administração terá o prazo de até 30 (trinta) dias corridos a contar da

data do protocolo do requerimento, tratado no item 10.1.10, para decidir e admitir a prorrogação motivada por igual período, conforme art. 123, Lei Federal nº 14.133, de 2021.

10.1.11. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo Contratado no prazo máximo de [inserir prazo] ([inserir prazo por extenso]) dias corridos.

10.1.12. Aplicar ao Contratado as sanções legais e regulamentares.

10.1.13. Exigir o cumprimento dos recolhimentos tributários, trabalhistas e previdenciários por meio dos documentos pertinentes.

10.1.14. Disponibilizar local adequado para a realização do serviço.

10.1.15. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

10.1.16. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

10.1.17. [Podem ser incluídas outras obrigações que forem necessárias a depender da especificidade do objeto].

10.2. **Do Contratado**:

10.2.1. O Contratado deve cumprir todas as obrigações constantes deste instrumento e seus anexos, nas quantidades, prazos e condições pactuadas, assumindo exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

10.2.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor, Lei Federal nº 8.078, de 1990.

10.2.3. Comunicar ao Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

10.2.4. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior, conforme inciso II, art. 137 da Lei Federal nº 14.133, de 2021, e inciso III, art. 16 do Decreto nº 48.587, de 2023, e prestar todo esclarecimento ou informação por eles solicitados.

10.2.5. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou dos materiais nela empregados.

10.2.6. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos.

10.2.7. Arcar com os descontos nos pagamentos ou garantia, se for o caso, do valor correspondente aos danos sofridos, devidamente comprovados.

10.2.8. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do Contratante ou do fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei Federal nº 14.133, de 2021.

10.2.9. Emitir faturas no valor pactuado, apresentando-as ao Contratante para ateste e pagamento;

10.2.10. Responsabilizar-se pela garantia dos materiais empregados nos serviços prestados, dentro dos padrões adequados de qualidade, segurança, durabilidade e desempenho,

conforme previsto na legislação em vigor e na forma exigida neste Termo de Referência.

10.2.11. Manter, durante toda a execução do objeto, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação.

10.2.12. Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante e não onerará o objeto do contrato.

10.2.13. Comunicar ao fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual.

10.2.14. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

10.2.15. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

10.2.16. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas, conforme art. 116 da Lei Federal nº 14.133, de 2021.

10.2.16.1. Comprovar a reserva de cargos a que se refere a cláusula acima, quando solicitado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas, conforme parágrafo único, art. 116 da Lei Federal nº 14.133, de 2021.

10.2.17. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

10.2.18. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no inciso II, alínea “d”, art. 124 da Lei Federal nº 14.133, de 2021.

10.2.19. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante.

10.2.20. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste documento, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência.

10.2.21. Orientar e treinar seus empregados sobre os deveres previstos na Lei Federal nº 13.709, de 2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução do objeto contratado.

10.2.22. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina.

10.2.23. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

10.2.24. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

11. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

11.1. Comete infração administrativa, nos termos da Lei Federal nº 14.133, de 2021, o Contratado ou o licitante que:

11.1.1. Der causa à inexecução parcial da contratação;

11.1.2. Der causa à inexecução parcial da contratação que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

11.1.3. Der causa à inexecução total da contratação;

11.1.4. Deixar de entregar a documentação exigida para o certame;

11.1.5. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

11.1.6. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

11.1.7. Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

11.1.8. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a contratação e a execução do contrato;

11.1.9. Fraudar a licitação ou praticar ato fraudulento na execução da contratação;

11.1.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

11.1.11. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

11.1.12. Praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846, de 2013.

11.2. Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

11.2.1. **Advertência** - quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave, conforme disposto no § 2º, art. 156 da Lei Federal nº 14.133, de 2021;

11.2.2. **Impedimento de licitar e contratar** - quando praticadas as condutas descritas nos subitens 11.1.2 a 11.1.7, sempre que não se justificar a imposição de penalidade mais grave, conforme disposto no § 4º, art. 156, da Lei Federal nº 14.133, de 2021;

11.2.3. **Declaração de inidoneidade para licitar e contratar** - quando praticadas as condutas descritas nos subitens 11.1.8 a 11.1.12, bem como nos subitens 11.1.2 a 11.1.7, que justifiquem a imposição de penalidade mais grave, conforme disposto no § 5º, art. 156, da Lei Federal nº 14.133, de 2021).

11.2.4. **Multa**:

11.2.4.1. Moratória de [inserir percentual]% ([inserir percentual por extenso]) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de [inserir número de dias] ([escrever por extenso]) dias.**OU**

11.2.4.1 Moratória de [inserir percentual]% ([inserir percentual por extenso]) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de [inserir percentual]% ([inserir percentual por extenso]), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.

I - O atraso superior à [inserir número de dias] ([escrever por extenso]) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei Federal nº 14.133, de 2021.

11.2.4.2. Compensatória, para as infrações descritas nos subitens [descrever o item], de [inserir percentual] % ([inserir percentual por extenso]) a [inserir percentual] % ([inserir percentual por extenso]) do valor da contratação.

11.3. As sanções previstas nos subitens 11.2.1, 11.2.2 e 11.2.3 poderão ser aplicadas cumulativamente com a multa, conforme disposto no § 7º, art. 156, da Lei Federal nº 14.133, de 2021.

11.4. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento

eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente, conforme § 8º, art. 156, da Lei Federal nº 14.133, de 2021.

11.5. A aplicação das sanções previstas neste documento não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante, conforme disposto no § 9º, art. 156, da Lei Federal nº 14.133, de 2021.

11.6. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, conforme disposto no art. 157, da Lei Federal nº 14.133, de 2021.

11.7. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de [inserir número de dias] ([escrever por extenso]) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

11.8. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei Federal nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

11.9. Em observância ao disposto no § 1º, art. 156, da Lei Federal nº 14.133, de 2021, na aplicação das sanções serão considerados:

11.9.1. A natureza e a gravidade da infração cometida;

11.9.2. As peculiaridades do caso concreto;

11.9.3. As circunstâncias agravantes ou atenuantes;

11.9.4. Os danos que dela provierem para a Administração Pública;

11.9.5. A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

11.10. Os atos previstos como infrações administrativas na Lei Federal nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei Federal nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos no art. 159 da referida Lei de Licitações.

11.11. A personalidade jurídica do Fornecedor poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste documento ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia, conforme disposto no art. 160, da Lei Federal nº 14.133, de 2021.

11.12. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal, conforme art. 161, da Lei Federal nº 14.133, de 2021.

11.13. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei Federal nº 14.133, de 2021.

11.14. Os débitos do Contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora contratante.

12. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

12.1. O custo estimado da contratação possui caráter sigiloso e será tornado público após o julgamento das propostas.

13. ADEQUAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes da presente contratação correrão por conta da dotação orçamentária do orçamento em vigor, aprovado pela Lei 25.124 de 30 de dezembro de 2024:

13.1.1. A contratação será atendida pela seguinte dotação: 1191 04 126 033 2006 0001 3390 4002, fontes 10.1 e /ou 29.1.

13.2. A dotação relativa ao exercício financeiro subsequente será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

14. TERMO DE SIGILO E CONFIDENCIALIDADE:

14.1. Juntamente com o contrato de fornecimento deverá ser assinado Termo de Sigilo e Confidencialidade padrão da SEF/MG. O Termo de Confidencialidade é necessário por questão de segurança do negócio da SEF/MG. As informações originadas e tramitadas na prestação de serviços de comunicação do presente objeto são, em quase sua totalidade, sigilosas, portanto, faz-se imprescindível a previsão de celebração de Termo de Confidencialidade neste processo.

[Inserir nome completo]

Masp

Responsável pela Elaboração

Rogério Zupo Braga

Masp 668.359-3

Masp

Responsável pela Aprovação

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 10:57, 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 **112440727** e o código CRC **9B978BBA**.