GOVERNO DO ESTADO DE MINAS GERAIS

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS

Assessoria de Tecnologia da Informação

TERMO DE REFERÊNCIA

DATA	ÓRGÃO SOLICITANTE	NÚMERO DA UNIDADE DE COMPRA
14/05/2025	IPSM	2121022

RESPONSÁVEL PELA SOLICITAÇÃO	SUPERINTENDÊNCIA OU DIRETORIA OU UNIDADE ADMINISTRATIVA
Nome: Mônica Cristina dos Santos E-mail: monica.santos@ipsm.gov.br	DG

SUMÁRIO

1. OBJETO E CONDIÇÕES GERAIS DA CONTRATAÇÃO

O presente Termo de Referência tem por objeto a **contratação de empresa especializada para fornecimento, implantação e suporte de solução integrada de Firewall de Aplicação Web (WAF) do fabricante F5 Networks, plataforma BIG-IP Virtual Edition Advanced WAF versão V23, contemplando balanceamento de carga de aplicações, subscrições, suporte técnico do fabricante e serviços especializados de instalação, configuração, ativação e colocação em produção, pelo período de 12 (doze) meses**, nos termos da tabela abaixo e conforme condições e exigências estabelecidas neste documento.

1.1. Dos serviços a serem prestados:

O referido OBJETO contempla o serviço de suporte técnico, incluindo manutenção corretiva, pelo período de 12 (doze) meses, conforme tabela abaixo:

LOTE ÚNICO							
Item	**Código do item**	**El-item**	**Discriminação do Serviço**	**Execução**	**Quantidade**	**Preço unitário**	**Valor total**
01	000103560	4002	Appliance Virtual para WAF – Web Application Firewall com Balanceamento de Carga de Aplicações, IP Intelligence e Threat Campaigns, com subscrições e suporte do fabricante por 1 (um) ano. Fabricante: F5 Networks. Modelo: BIG-IP VE 1G	Única	01	R$ 265.490,00	R$ 265.490,00
02	000138029		Serviços técnicos especializados de instalação, configuração, ativação e colocação em produção	Única	01	R$ 16.780,00	R$ 16.780,00
TOTAL GERAL							**R$ 282.270,00**

1.2. Caracterização do objeto:

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:

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 **12 (doze) meses**, contado do primeiro dia útil subsequente à divulgação no Portal Nacional de Contratações Públicas (PNCP), com previsão de início em **25/06/2026** e término em **24/06/2027**, prorrogável por até, no máximo, **10 (dez) anos**, na forma dos arts. 106 e 107 da Lei Federal nº 14.133, de 2021.

1.4.1.1. A presente prestação de serviço é enquadrada como **continuada**, sendo a vigência plurianual mais vantajosa para a Administração.

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

1.4.3. Encerrado o procedimento licitatório, o representante legal da licitante declarada vencedora será convocado para firmar o termo de contrato de acordo com o art. 95 da Lei Federal nº 14.133/2021.

1.4.4. A prorrogação citada no subitem 1.4.1 ocorrerá caso sejam preenchidos, de forma simultânea, os requisitos abaixo enumerados, e autorizado formalmente pela autoridade competente:

1.4.4.1. Prestação regular dos serviços;

1.4.4.2. Não aplicação de punições de natureza pecuniária por 3 (três) vezes ou mais, exceto quanto a penalidades aplicadas por atraso na entrega da garantia;

1.4.4.3. Manutenção do interesse pela CONTRATANTE na realização do serviço;

1.4.4.4. Manutenção da vantajosidade econômica do valor do contrato para a administração; e

1.4.4.5. Concordância expressa da CONTRATADA pela prorrogação.

2. DESCRIÇÃO DA SOLUÇÃO

ITEM 1 - Solução integrada de segurança de Data Center WAF (WEB APPLICATION FIREWALL)

2.1. A solução atualmente utilizada pelo IPSM é composta pela plataforma BIG-IP Virtual Edition da fabricante F5 Networks, responsável pela proteção das aplicações web institucionais, balanceamento de carga entre servidores, inspeção de tráfego criptografado, mitigação de ameaças cibernéticas e manutenção da disponibilidade dos serviços tecnológicos disponibilizados pelo IPSM.

2.2. Considerando a descontinuidade da versão atualmente utilizada, bem como a impossibilidade de renovação do suporte técnico e garantia do fabricante, a presente contratação contempla a modernização da solução existente, mediante fornecimento de nova versão da plataforma BIG-IP Virtual Edition Advanced WAF V23, incluindo funcionalidades avançadas de proteção de aplicações, inteligência contra ameaças, balanceamento inteligente de carga e demais recursos de segurança necessários à continuidade operacional do ambiente tecnológico institucional.

2.3. A solução deverá contemplar, no mínimo, as características técnicas e funcionalidades descritas a seguir:

2.4. **Características Gerais:**

2.4.1. Não serão aceitos produtos ou serviços do tipo demo, trial e open-source. A solução deve ser do fabricante F5 Networks devido à compatibilidade técnica com o ambiente atualmente em uso.

2.4.2. A solução de WAF deve ser fornecida em appliance virtual, e deve prover todas as funcionalidades e recursos descritos nessa especificação técnica. O nome de cada licenciamento de software do fabricante F5 que compõe a solução deve estar descrito na proposta comercial, sob pena de desclassificação.

2.4.3. O appliance virtual deve ser compatível com e rodar em Nutanix AHV além de estar disponível no marketplace da AWS, GCP e Azure para contratação no modelo Bring Your Own License (BYOL).

2.4.4. A solução deve ser capaz de visualizar, via console, as informações de saúde e desempenho de todo o ambiente que a compõem, incluído softwares e equipamentos.

2.4.5. Possuir suporte a SNMP v2c e v3.

2.4.6. Enviar mensagens por e-mail e traps SNMP.

2.4.7. Os componentes da solução poderão ser executados num mesmo appliance, ou poderão ser distribuídos em múltiplos appliances, de acordo com a característica de cada produto, respeitadas as características de funcionamento e performance exigidas neste Termo de Referência.

2.4.8. A solução deve ter o pleno funcionamento independentemente de conexão (física ou lógica) com o fabricante, exceto para atualizações de versões e de segurança.

2.4.9. Suportar IPV6.

2.4.10. A solução deve possuir a capacidade para suportar a adição de novos componentes (hardware e/ou software) escaláveis sem causar interrupções no funcionamento da solução.

2.4.11. Apresentar uma relação descritiva dos componentes fornecidos, incluindo seus códigos comerciais.

2.4.12. Não será aceito equipamento do tipo NGFW (Next Generation Firewall)

2.5. **Características do Appliance:**

2.5.1. Deve ser capaz de executar todas as suas funções de aprendizado, análise e proteção de tráfego web considerando pelo menos uma taxa de transferência de 1 (um) Gbps.

2.5.2. A solução deve ter vários mecanismos de implantação (deployment) com pelo menos uma ponte transparente na linha (Bridge L2), Proxy Reverso. Deve possuir a capacidade de monitorar e auditar todos os acessos de modo (passivo) a fim de monitorar o tráfego sem fazer alterações na rede.

2.5.3. A solução deve permitir a integração nos modos proxy reverso explícito e proxy reverso transparente (Bridge L2).

2.5.4. A solução deve ter um impacto de milissegundos na latência da rede.

2.5.5. O sistema deve permitir a integração e envio de alertas para terceiros ou ferramentas de correlação (SIEM). Será permitido que a integração seja realizada através da exportação de eventos utilizando SYSLOG ou através de RestAPI.

2.5.6. O produto deve suportar o protocolo de gerenciamento de rede SNMP a ser monitorado por ferramentas de terceiros.

2.5.7. A solução de WAF com balanceamento de carga de aplicações devem ser do mesmo fabricante e ser uma única solução integrada, não sendo aceita a composição de produtos distintos.

2.5.8. A capacidade de processamento da solução deve seguir as melhores práticas do fabricante, considerando todos os requisitos de capacidade definidos nesta especificação, tais como: tráfego, conectividade, conexões, requisições nível 7, requisições SSL, transações e compressão.

2.5.9. Deve possui CPU e memória suficientes para atender os throughputs definidos neste Termo de Referência, tanto para WAF quanto para o balanceador sem degradação de performance da solução quando ativada simultaneamente as duas funcionalidades.

2.5.10. O appliance virtual que será responsável pela inspeção de tráfego web e pelo balanceamento de carga e deve suportar o throughput de pelo menos 1 (um) Gbps tanto para a funcionalidade de firewall de aplicação Web como para a funcionalidade de balanceamento de carga entre aplicações.

2.6. **Balanceamento, Cache e Aceleração Web:**

2.6.1. Deve suportar no mínimo 1 (um) Gbps de inspeção de tráfego na camada 7. Para alcançar esse throughput será aceito que o equipamento faça cache, em

memória RAM ou SSD, do conteúdo estático, como por exemplo imagens, após a sua primeira inspeção. Todo conteúdo estático permitido em cache não será reinspecionado até a expiração do cache;

2.6.2. A solução fornecida deve ser capaz de operar em cluster, oferecendo alta disponibilidade com tolerância a falhas, independentemente da quantidade de elementos que componham o cluster. Apenas um appliance está sendo requerido neste Termo de Referência;

2.6.3. Na falha de um dos elementos do cluster, não poderá haver nenhuma degradação ou indisponibilidade das aplicações;

2.6.4. Deve suportar configuração de mTLS em um virtual server;

2.6.5. Deve suportar configuração de mTLS por url e path de aplicação;

2.6.6. A solução deve ser capaz de trabalhar com recursos de alta disponibilidade, permitindo a ligação de dois ou mais equipamentos possibilitando configurar um único IP dos recursos protegidos nos dois ou mais equipamentos;

2.6.7. Deve ser fornecido todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais;

2.6.8. A solução deve permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

2.6.8.1. Compartilhar a rede de heartbeat com a rede de dados;

2.6.8.2. Utilizar uma rede exclusiva para o heartbeat;

2.6.9. A solução deve ser capaz de trabalhar no modo Ativo/Standby, com equipamento de mesmo fabricante, em caso de futuras expansões;

2.6.10. A solução deve ser capaz de trabalhar no modo Ativo/Ativo, mantendo o status das conexões, em caso de operação conjunta com outro appliance do mesmo fabricante;

2.6.11. Aceita-se como Ativo-Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e em espera no outro;

2.6.12. A solução deve suportar múltiplas tabelas de rotas independentes;

2.6.13. O appliance, quando habilitado para mais de uma função (Server Load Balancing (SLB), Aceleração Web, etc.), deve permitir a definição da importância da função, determinando quantidade de processamento (CPU e memória) serão alocados para cada tipo de funcionalidade.

2.6.14. A solução deve possuir capacidade para gerenciar os recursos dispon;veis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, aceleração Web, etc;

2.6.15. A solução deve suportar e estar licenciado para todas as aplicações comuns de um Switch Layer 7 (sete):

a) Server Load-Balancing;

b) Firewall Load-Balancing;

c) Proxy Load-Balancing.

2.6.16. A solução deve possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;

2.6.17. Suportar balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

2.6.18. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

2.6.19. A solução deve ser capaz de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;

2.6.20. A solução deve suportar e estar licenciada para os seguintes métodos de balanceamento:

a) Round Robin;

b) Least Connections;

c) Weighted Percentage (por peso);

d) Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

e) Weighted Percentage dinâmico (baseado no número de conexões);

f) Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI.

2.6.21. A solução deve ser capaz de balancear as novas sessões, preservando as sessões existentes no mesmo servidor e implementando persistência de sessão dos seguintes tipos:

a) Por cookie – inserção de um novo cookie na sessão;

b) Por cookie – utilização do valor do cookie da aplicação, sem adição de cookie;

c) Por endereço IP destino;

d) Por Endereço IP origem;

e) Por sessão SSL;

f) Através da análise da URL acessada;

g) Através da análise de qualquer parâmetro no header HTTP;

h) Através da análise de qualquer informação da porção de dados (camada 7).

2.6.22. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH ou utilizando algum protocolo ou solução similar.

2.6.23. A solução deve suportar os seguintes métodos de monitoramento dos servidores reais:

a) Layer 3 – ICMP;

b) Conexões TCP e UDP pela respectiva porta no servidor;

2.6.24. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, FTP, SMB, RADIUS, NNTP, RPC, LDAP, IMAP, SMTP, POP3, SIP, SOAP, SNMP. Caso não exista um monitor pré-definido deve ser possível criar um monitor de forma manual.

2.6.25. A solução deve possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico.

2.6.26. A solução deve possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual.

2.6.27. A solução deve possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores.

2.6.28. A solução deve possuir as seguintes funcionalidades de segurança ativas e licenciadas:

a) Network Address Translation (NAT);

b) Proteção contra Denial of Service (DoS);

c) Proteção contra Syn flood;

d) Implementar Listas de Controle de Acesso (ACL);

e) Permitir o controle da resposta ICMP por servidor virtual;

f) Realizar Limpeza de cabeçalho HTTP;

g) Análise em Camada 7 de Protocolos, com alertas para violações na camada de Protocolo HTTP.

2.6.29. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente.

2.6.30. Deve ser possível definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate).

2.6.31. Deve ser possível definir compressão especificamente para certos tipos de objetos.

2.6.32. A solução deve possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia.

2.6.33. A solução deve ser capaz de ser configurada para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado.

2.6.34. Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores.

2.6.35. Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados.

2.6.36. Garantir que o recurso de cache possa ajustado em relação a quantidade de memória que será utilizada para armazenar objetos.

2.6.37. Possuir a capacidade para determinar qual o tamanho máximo do objeto a ser cacheado.

2.6.38. Possuir a capacidade para determinar qual o tamanho do menor objeto a ser cacheado.

2.6.39. Possuir a capacidade para determinar a URI (Uniform Resource Identifiers) que deve ser cacheada.

2.6.40. Possuir a capacidade para ler, alterar e ignorar o parâmetro cache-control no cabeçalho HTTP.

2.6.41. Possuir a capacidade para inserir e alterar o parâmetro age header no cabeçalho HTTP.

2.6.42. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor.

2.6.43. A solução deve suportar Internet Content Adaptation Protocol (ICAP).

2.6.44. Deve ser capaz de realizar DHCP relay.

2.6.45. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas.

2.6.46. A Solução deve ter suporte a sFlow.

2.6.47. A solução deve ter suporte a, no mínimo, TLS 1.2, SHA 2 Cipher e SHA256 hash.

2.6.48. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deve descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores

2.6.49. Deve ser possível configurar o tamanho máximo da fila.

2.6.50. Deve ser possível configurar o tempo máximo de permanência na fila.

2.6.51. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede.

2.6.52. A solução deve realizar Controle de Banda Dinâmico para grupos de aplicações e rede.

2.6.53. A solução deve realizar Controle de Banda baseado em domínio de roteamento.

2.6.54. A solução deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.

2.6.55. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra-ataques;

2.6.56. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores: GEOIP, http-basic-auth, http-cookie, http-header, httphost, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version.

a) Deve ser possível tomar as seguintes ações através dessas políticas:

b) Bloqueio de tráfego;

c) Reescrita e manipulação de URL;

d) Registro de tráfego (log);

e) Adição de informação no cabeçalho HTTP;

f) Redirecionamento do tráfego para um membro específico;

g) Selecionar uma política específica para Aplicação Web.

h) Devera possuir inteligência artificial para detecção além das assinaturas pré-definidas.

2.7. **Características de Proteção de aplicações Web:**

2.7.1. A solução pode executar automaticamente varreduras de rede que permitem a descoberta de novos servidores e serviços nos protocolos HTTP e HTTPS.

2.7.2. A solução deve proteger a infraestrutura web das aplicações de ataques contra a camada de aplicação (Camada 7).

2.7.3. A solução deve fornecer a possibilidade de bloquear transações WEB de maneira preventiva, antes que elas cheguem via rede ao servidor.

2.7.4. Deve ser capaz de correlacionar eventos ou violações de políticas.

2.7.5. A solução deve detectar, alertar e bloquear opcionalmente, em tempo real, qualquer comportamento malicioso conhecido e/ou desconhecido.

2.7.6. A solução deve ter um modo de aprendizado que permita definir quais ações são esperadas e aceitas pelos usuários.

2.7.7. No modo de aprendizado, o sistema deve aprender a estrutura e os elementos do aplicativo e essas informações devem estar disponíveis para automatizar a configuração do modelo de segurança positivo. Pelo menos você deve aprender sobre: Hosts válidos, URLs, parâmetros, cookies, tipo de conteúdo dos parâmetros

2.7.8. No modo de aprendizado, deve aprender além do comportamento esperado do usuário e essas informações devem estar disponíveis para automatizar a configuração do modelo de segurança positivo. No mínimo, você deve aprender sobre: Caracteres aceitos, tamanho do valor esperado.

2.7.9. O modo de aprendizagem pode ser ativado e desativado manualmente para estender o tempo de reconhecimento do padrão de comportamento.

2.7.10. O modo de aprendizagem deve poder permanecer ativo mesmo quando está em modo de proteção ou bloqueio, permitindo a incorporação de novos parâmetros ou características do mesmo sem ter que fazê-lo manualmente. De tal forma que a configuração de segurança positiva é atualizada automaticamente e constantemente.

2.7.11. Com relação a quaisquer ataques ou outra atividade não autorizada, a solução deve ser capaz de tomar as medidas adequadas, pelo menos: Terminar solicitações e respostas, bloquear a sessão TCP, colocados em quarentena temporária ou bloquear o usuário do aplicativo, colocar em quarentena temporária ou bloquear o endereço IP de origem.

2.7.12. A solução deve ter um conjunto de padrões correspondentes aos ataques conhecidos. Esta base de dados de padrões deve poder ser atualizada periodicamente, automaticamente e sem ajuda.

2.7.13. A solução deve permitir a definição para as regras e alarmes, condições lógicas em que o alarme ou o bloqueio não sejam ativos se não aconteceu o

evento, pelo menos, um número de vezes definido dentro de um período de tempo definido e associado a um contexto de conexão definível.

2.7.14. A solução deve ter a capacidade de proteger os serviços Web com base no SOAP.

2.7.15. A solução deve ter a capacidade de receber e usar certificados e pares de chaves pública / privada para servidores da Web protegidos.

2.7.16. A solução deve poder inspecionar e monitorar todos os dados HTTP/S do aplicativo, incluindo cabeçalhos HTTP, campos de formulário e o corpo de solicitações HTTP/S.

2.7.17. A solução deve inspecionar as solicitações e as respostas HTTP/S.

2.7.18. A solução deve ser capaz de validar todos os tipos de dados inseridos, incluindo URLs, formulários, cookies, consultas, campos e parâmetros ocultos, métodos HTTP, elementos XML e ações SOAP.

2.7.19. A solução deve ser capaz de identificar o usuário do aplicativo da Web. A identificação deve persistir até que o usuário tenha deixado o aplicativo.

2.7.20. A solução deve ser capaz de identificar e manter um registro das sessões da Web no nível do aplicativo, por meio de cookies de rastreamento ou parâmetros do aplicativo.

2.7.21. A solução deve ser capaz de aplicar uma correção virtual (virtual patching) para proteger as vulnerabilidades detectadas e deve ter integração com scanners de vulnerabilidade (pelo menos 3 soluções ou serviços diferentes do mercado) para receber os seus resultados ou relatórios, interpretar e sugerir mudanças para aplicar como correção virtual.

2.7.22. A solução deve suportar a detecção de ferramentas de download automático, bots, scripts, etc. através da geração de um requisito em JavaScript, a fim de bloquear todas as consultas que não possuem um navegador real por trás.

2.7.23. A solução deve ser capaz de implementar controles anti-scrapping de forma nativa, permitindo bloquear tentativas automatizadas de roubar informações do site.

2.7.24. A solução deve ser capaz de reconhecer IPs de fontes mal-intencionadas (como redes TOR, proxies anônimos, sites de Phishing, etc.) e também ter catalogação de IPs por geolocalização. Essas informações devem ser atualizadas periodicamente e deve ser possível integrar políticas de segurança como um critério.

2.7.25. A solução deve fornecer proteção automatizada para todas as vulnerabilidades expressas no OWASP Top 10.

2.7.26. A solução deve permitir a geração de exceções para as políticas de segurança de validação de protocolo por URL ou IP de origem.

2.7.27. A solução deve permitir a inspeção das conexões SSL (SSL v3, TLS v1) implementadas nos servidores da web. Para isso, os certificados (chave pública e privada) podem ser importados.

2.7.28. A solução deve validar se o conteúdo e a duração do protocolo HTTP, incluindo os cabeçalhos, corpo e cookies, estão corretos. Por sua vez, você deve ser capaz de restringir os métodos HTTP usados em um aplicativo da Web (GET, POST, PUT, etc.).

2.7.29. A solução deve permitir ações e alertar para violações de protocolos inferiores ao aplicativo, incluindo inspeção de pacotes IP, TCP, UDP e seus cabeçalhos.

2.7.30. A solução deve proteger os aplicativos da Web contra-ataques comuns, como:

a) njeção SQL (SQL Injection).

b) Injeção de LDAP (LDAP Injection).

c) Comando do SO (SO Commanding).

d) Injeção SSI (SSI Injection).

e) Inclusão remota de arquivos (Remote File Inclusion).

f) Mail Command Injection.

g) Injeção de XML (XML Injection).

h) Injeção Xpath (XPath Injection).

i) Injeção Xquery (XQuery Injection).

j) Cross Site Scripting (XSS).

k) Cross Web Request Forgery (CSRF).

l) Web Scrapping.

m)Navegação forçada (Forceful Browsing).

2.7.31. Proteção de modificação de campos ocultos.

2.7.32. Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes.

2.7.33. A solução deve suportar a definição de políticas diferentes que podem ser associadas a cada aplicativo individualmente.

2.7.34. Para cada aplicação protegida, o administrador deve ser capaz de configurar em que momento é feita a detecção (log) dos ataques recebidos e quando eles evitam (bloqueiam) os ataques.

2.7.35. Para cada aplicativo da Web, deve ser possível desabilitar a prevenção de ataques (bloqueio) e deixar apenas a detecção (log) em formato granular para facilitar a solução de problemas por tipos de ataques.

2.7.36. No caso de um bloqueio, dependendo do modo de operação, a resposta (página) enviada ao usuário deve poder ser personalizada.

2.7.37. A solução deve permitir que hosts ou clientes confiáveis sejam excluídos das medidas de proteção.

2.7.38. A solução deve suportar a identificação do IP de origem no caso de passar por proxy, interpretando o campo X-forwarded-for do cabeçalho HTTP.

2.7.39. A solução deve validar se o conteúdo e a duração do protocolo HTTP, incluindo os cabeçalhos, corpo e cookies, estão corretos.

2.7.40. Deve possuir hardware dedicado para inspeção otimizada de tráfego criptografado com SSL e TLS.

2.7.41. A latência inserida no tráfego SSL não pode superar os 5ms (cinco milissegundos).

2.7.42. Deve possuir a certificação ICSA Labs para Firewall de Aplicação (Web Application Firewall).

2.7.43. A solução deve suportar o uso de firewall camada 3 e 4 junto com firewall camada 7 no mesmo appliance para evitar problemas com o aumento da latência.

2.7.44. A solução deve suportar responder por 1 endereço IP e vários endereços IPs por aplicação web.

2.7.45. Deve poder atuar como Web Application Firewall em modo WAF Positivo (permitindo apenas o que é conhecido e esperado).

2.7.46. Deve poder atuar como Web Application Firewall em modo WAF Negativo (bloqueando características conhecidas de ataque).

2.7.47. Deve ser capaz de operar usando modelo positivo de segurança, por meio de aprendizado e de definição de regras que descrevem o comportamento esperado de um aplicativo ou serviço, efetuando o bloqueio de todo o tráfego que não coincide com essas regras (árvore de acesso válido).

2.7.48. Possuir as seguintes características:

2.7.49. Facilidade para liberação de regras aprendidas automaticamente que estejam gerando grande quantidade de falso positivo;

2.7.50. Facilidade para transformar um ataque detectado e considerado falso positivo como regra do firewall;

2.7.51. Facilidade para aplicar diferentes regras para diversas aplicações;

2.7.52. Capacidade para customizar regras de negação de serviço;

2.7.53. Capacidade para combinar detecção e prevenção na construção das regras;

2.7.54. Capacidade para desfazer a aplicação de uma regra.

2.7.55. Deve suportar o modelo de segurança positivo, devendo ser capaz de aprender qual perfil de tráfego é legítimo e bloquear ataques ou atividades não autorizadas.

2.7.56. Deve possuir políticas de segurança de aplicações web pré-configuradas na solução.

2.7.57. Deve permitir a criação de políticas diferenciadas por aplicação.

2.7.58. Deve possuir funcionalidade que ajuste dinamicamente o nível de proteção na detecção de ataques.

2.7.59. Deve ser possível utilizar uma política em múltiplas aplicações (uma para várias).

2.7.60. Deve ser possível utilizar uma política para cada aplicação (uma para uma).

2.7.61. Deve possuir funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação.

2.7.62. O perfil aplicação aprendido de forma automatizada pode ser ajustado, editado ou bloqueado.

2.7.63. Deve identificar e criar um perfil de utilização das aplicações, mesmo que as páginas Web e conteúdos sejam dinâmicos, como os desenvolvidos em JavaScript, CGI, ASP, PHP e Java.

2.7.64. Deve suportar WebSocket Traffic Filter.

2.7.65. Deve suportar o controle de política granular baseada no caminho do aplicativo (application path).

2.7.66. Deve permitir a aceitação de falsos positivos (exceção à política de segurança).

2.7.67. Deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente.

2.7.68. Deve suportar a configuração de hosts confiáveis para permitir a execução de operações não permitidas pela política adotada para uso em eventos de testes de penetração, solução de problemas (troubleshooting) e análise de performance.

2.7.69. Deve possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos.

2.7.70. Deve ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção à regra geral.

2.7.71. As atualizações de assinaturas deverão passar por um período configurável de testes, onde nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura.

2.7.72. A solução deve realizar bloqueios de ataques mesmo sem assinaturas atualizadas.

2.7.73. Deve implementar consultas a bases de reputação externas;

2.7.74. A solução deve ser capaz de decifrar tráfego SSL a partir da importação de chaves criptográficas, para permitir a inspeção de todo conteúdo do pacote originalmente cifrado.

2.7.75. Inspeção de tráfego através da troca de chaves assimétricas entre cliente e WAF (proxy SSL).

2.7.76. A solução deve suportar SSL Offload de conexões.

2.7.77. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação. Essa inspeção poderá ser feita via integração ICAP.

2.7.78. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação.

2.7.79. Permitir a integração com Firewall de Database de outros fabricantes.

2.7.80. Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtrar relatórios por IDs de dispositivos.

2.7.81. A solução deve permitir proteção contra envio de arquivos, considerando tamanho e tipo.

2.7.82. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra-ataques recentes.

2.7.83. A solução deve se integrar com outras soluções de segurança como firewall, IPS e análise de logs de outros fabricantes.

2.7.84. Deve armazenar os logs localmente ou exportar para Syslog server.

2.7.85. Possuir registro de logs com as seguintes características:

a) Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;

b) Os registros de log de acesso e eventos devem ser armazenados em arquivo ou em banco de dados que permita a exportação ou em outro formato aberto como CSV ou TXT, podendo ainda serem armazenados localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em servidor externo de banco de dados;

c) Permitir configurar a retenção dos logs por tempo e volume;

d) Ter capacidade para detecção, remoção ou codificação de dados sensíveis do log.

2.7.86. Deve ser capaz de diferenciar acessos entre bots, Web scraping e usuários humanos para bloquear ataques automatizados.

2.7.87. Deve oferecer um serviço baseado na reputação do endereço IP de origem, protegendo as aplicações de serem acessadas pelas seguintes origens: Rede TOR, proxies anônimos e endereços IP de baixa reputação.

2.7.88. A Solução de Firewall de Aplicação deve suportar diferentes métodos de autenticação dos usuários das aplicações como: HTML Form, HTTP Basic Authentication, JSON/AJAX Request, NTLM, certificados SSL Client e HTTP Digest Authentication.

2.7.89. A solução deve ser capaz de identificar e bloquear ataques através de:

a) Assinaturas, com atualização periódica da base pelo fabricante;

b) Regras de verificação personalizadas – política de segurança configurada.

2.7.90. Comportamento malicioso.

2.7.91. Deve trabalhar com filtros de segurança:

a) De controle dos parâmetros das aplicações;

b) De proteção a sessão;

c) De controle de vulnerabilidades;

d) De controle de serviços Web;

e) De proteção a XML.

2.7.92. Permitir o bloqueio de ataques dos/DDoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio.

2.7.93. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser auto ajustáveis e adaptáveis de acordo com mudanças.

2.7.94. Possuir as seguintes formas de detecção de ataques dos/DDoS na camada de aplicação:

2.7.95. Número de requisições por segundo enviados a uma URL específica;

2.7.96. Número de requisições por segundo enviados de um IP específico;

2.7.97. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);

2.7.98. Número máximo de transações por segundo (TPS) de um determinado IP;

2.7.99. Aumento de um determinado percentual do número de transações por segundo (TPS);

2.7.100. Aumento do tempo de resposta (latência de aplicação) de uma determinada URL.

2.7.101. Deve permitir criar lista de exceção (whitelist) por endereço IP específico ou faixa de sub-rede.

2.7.102. Permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.

2.7.103. Deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual.

2.7.104. Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período de tempo determinado através de configuração.

2.7.105. Permitir o bloqueio de determinados endereços IPs que ultrapassarem um número máximo de violações por minuto. O período de bloqueio deve ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente.

2.7.106. A solução deve permitir o cadastro de robôs que podem acessar a aplicação.

2.7.107. Deve permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais.

2.7.108. Deve possuir mecanismo capaz de diferenciar entre bots e usuários humanos para bloquear ataques automatizados (robôs):

2.7.109. O mecanismo deve implementar mecanismos de desafios de Cookies, JavaScript e Captcha para reforçar a identificação de robôs;

2.7.110. O mecanismo deve consultar base de dados de robôs já conhecidos;

2.7.111. O mecanismo deve permitir a integração com o sistema de Captcha do Google.

2.7.112. Deve permitir adoção de critérios de decisão para bloqueio e alerta, considerando no mínimo 7 (sete) critérios simultâneos, dentre eles:

a) Tempo de resposta de uma página web;

b) Tamanho da resposta de uma página web;

c) User-agent (navegador);

d) Usuário;

e) IP de origem

f) País de origem

g) Assinatura de ataque;

h) Conteúdo do payload;

i) Conteúdo do cabeçalho;

j) Conteúdo do cookie;

k) Código de resposta do servidor web;

l) Nome do host (Host Header);

m) Número de ocorrências num intervalo de tempo;

n) Método HTTP;

o) Horário.

2.7.113. Ao detectar um ataque ou qualquer atividade não autorizada, deve ser possível bloquear:

a) Requisições e respostas;

b) Uma conexão TCP;

c) Uma rede específica;

d) Um endereço IP durante um intervalo de tempo específico.

2.7.114. A solução deve fornecer, para cada política de segurança, múltiplas opções de evento posteriores ao bloqueio da requisição, dentre eles: Enviar log para Syslog Externo, enviar um e-mail, alerta para a interface de monitoração da gerência, executar um script definido pelo administrador e apresentar uma página de erro para o usuário.

2.7.115. Quando uma requisição for bloqueada pelo WAF, deve ser possível comunicar ao usuário sobre o fato através de uma página HTML informativa.

2.7.116. Deve permitir a customização da resposta de bloqueio. Deve ser possível customizar a página HTML baseada em contextos como (Tipo de ataque, IP de Origem, Usuário e GeoLocalização) sendo configuradas através da GUI sem a necessidade de criação de scripts atém do HTML.

2.7.117. Deve implementar proteção ao JSON (JavaScript Object Notation), REST (Representational State Transfer) e SOAP (Simple Object Access Protocol).

2.7.118. Deve implementar proteção a API;

2.7.119. Deve implementar proteção WebSockets;

2.7.120. Deve implementar proteção sobre microservicos.

2.7.121. Deve possuir suporte a filtro e validação de funções XML específicas da aplicação.

2.7.122. Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais.

2.7.123. Deve prevenir que erros de aplicação ou infraestrutura sejam mostrados ao usuário.

2.7.124. A solução deve permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle.

2.7.125. A solução deve ser capaz de interpretar o campo X-Forwarded-For como endereço IP de origem original de um pacote, a fim de identificar a origem real de tráfego que sofra NAT de origem.

2.7.126. Deve proteger contra-ataques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas.

2.7.127. A Solução deve proteger, no mínimo, contra os ataques listados abaixo:

a) AJAX/JSON web threats;

b) Anonymous Proxy access

c) Application tampering;

d) Broken access control;

e) Buffer overflow;

f) Cross-site scripting (XSS);

g) Known Worms;

h) Malicious Encoding;

i) SQL injection;

j) Web Services (XML) attacks

k) XML bombs/DoS;

l) Brute force;

m) Cookie Injection;

n) Cookie manipulation;

o) Cookie poisoning;

p) Cross site request forgery (CSRF);

q) Directory Traversal;

r) Forceful browsing;

s) Hidden fields manipulation;

t) HTTP Denial of Service;

u) HTTP Response Splitting;

v) Illegal Encoding;

w) Layer 7 DoS and DDoS;

x) Malicious Robots;

y) OS Command Injection;

z) Parameter and HPP tampering;

aa) Remote File Inclusion;

ab) Request smuggling;

ac) Sensitive data Exposure;

ad) Session hijacking;

ae) Web scraping;

af) Web server software and operating system attacks;

2.7.128. Deve mitigar ataques de Slow HTTP.

2.7.129. A solução deve possuir lista dinâmica de endereços IP globais com atividades maliciosas.

2.7.130. A solução deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação.

2.7.131. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação.

2.7.132. Deve ajudar a prevenir contra-ataques de Credencial Stuffing, onde bases de credenciais expostas na Internet são usados para tentava de acesso de outras aplicações Web.

2.7.133. A solução deve ser capaz de inspecionar e bloquear solicitações XML, SOAP e HTTP (versões HTTP 1.0, 1.1 e 2.0).

2.7.134. A solução deve fazer checagem de:

a) Consistência de formulários;

b) Do cabeçalho do “user-agent” para identificar clientes inválidos;

c) Métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT), permitidos e bloqueados.

2.7.135. Deve dispor de bases de inteligência de IP, incluindo IPv4 e IPv6, classificados e categorizados em, pelo menos, as categorias fontes de ataques web, redes e hosts de botnets, scanners de websites, fontes de phishing, servidores proxies, redes e hosts que exploram vulnerabilidades em Windows, redes e hosts de negação de serviço e redes e hosts com baixa reputação;

2.7.136. Permitir que sejam criados filtros utilizando as categorias de IP nas funções de proteção de DDoS, de visibilidade de tráfego e de proteção de aplicações web e API;

2.7.137. Permitir utilizar a base de inteligência de IP para classificar e selecionar uma cadeia de serviço na solução de visibilidade de tráfego;

2.7.138. Permitir que sejam criados filtros onde se verifica o endereço de origem no cabeçalho X-Forwarded-For (XFF) com base na classificação de endereços IP na solução de proteção de aplicações web e API;

2.7.139. Dispor de base de inteligência de ameaças relacionados a campanhas e ataques a aplicações web, correlacionando diversas fontes de inteligência e ameaças encontradas diariamente no mundo real;

2.7.140. As regras de proteção e assinaturas derivadas desta base de inteligência devem ser habilitadas automaticamente, sem precisar de um ciclo de aprendizagem na solução;

2.7.141. A base de inteligência deve implementar detecção e mitigação de ataques com baixo índice de falso-positivo;

2.7.142. Este serviço é complementar a atualização de assinaturas de ataques da solução de proteção de aplicações web e API, portanto, as informações disponibilizadas pela base de inteligência não devem ser limitada a apenas indicar qual assinatura do WAF for acionada, devendo disponibilizar informações contextuais incluindo, por exemplo, a capacidade de informar que um agente conhecido de ameaça usou uma exploração específica de vulnerabilidade mais recente (por exemplo, um CVE) em uma tentativa de implantação de uma ameaça como, por exemplo, um software de mineração de criptomoedas;

2.8. **Gerenciamento:**

2.8.1. A solução deve ser gerenciada centralmente (configurações, controle e atualizações), através de interface web ou console de administração.

2.8.2. Possuir acesso controlado e autenticado por usuário, sendo que para a administração da solução deve-se usar uma conta para cada usuário administrador, independentemente da funcionalidade gerenciada.

2.8.3. O controle de acesso deve permitir a configuração de acesso por perfil às funções de Administração e Configuração de Regras.

2.8.4. Fornecer visualização e ações diferenciadas por perfis de acesso.

2.8.5. Permitir a visualização de painéis (dashboards).

2.8.6. Apresentar painéis gráficos (dashboards) com indicativos de situações diversas.

2.8.7. O equipamento deve fazer backup diário em forma automática de todas as informações nele armazenadas, incluindo as configurações de todos os módulos gerenciados e ter a capacidade de transferi-los automaticamente para um servidor remoto usando os protocolos SCP ou FTP.

2.8.8. Toda a configuração, administração e monitoramento da solução serão feitos através do console de administração.

2.8.9. A comunicação entre as estações de trabalho e o console de administração deve ser estabelecida através de um protocolo seguro com criptografia e autenticação por usuários locais, incluindo a possibilidade de usar certificados digitais.

2.8.10. A solução de administração deve permitir a atribuição de perfis de administração pelos usuários e esses perfis devem permitir a separação das funções de gerenciamento e monitoramento.

2.8.11. Capacidade de exportar logs para um formato SYSLOG ou SNMP TRAPS, para poder usar ferramentas de análise de terceiros.

2.8.12. O gerenciador deve possuir controle de interface gráfica Web (GUI: Graphical user interface) e interface por linha de comando (CLI – Command Line Interface).

2.8.13. A interface gráfica de gerenciamento deve ser cross-platform, em Web via protocolo HTTP e HTTPS, com suporte a acesso nativo via Microsoft Windows, Linux e Mac-OS.

2.8.14. Para interface gráfica do tipo Web, deve suportar no mínimo o navegador Mozilla Firefox e Chrome nas versões mais recentes.

2.8.15. A interface por linha de comando (CLI) deve possibilitar configuração dos equipamentos.

2.8.16. Deve possuir auto complementação de comandos;

2.8.17. Deve permitir acesso via SSH, criptografado;

2.8.18. Possuir um comando que mostre o tráfego de utilização das interfaces (bps e/ou pps);

2.8.19. Permitir reinicialização do equipamento;

2.8.20. Implementar Debugging: CLI via console e SSH;

2.8.21. A solução de gerenciamento deve possuir, no mínimo, três níveis de usuários: Administrador; Usuário com permissões reduzidas; e usuário Somente Leitura.

2.8.22. A solução de WAF e a solução de balanceamento de carga entre aplicações web deverão permitir que mais de um usuário possa estar conectado simultaneamente a interface de administração com a permissão de leitura/escrita.

2.8.23. A solução não deve ter nenhum limite de licença para a quantidade de usuários ou dispositivos que poderão ser configurados. O único limite que será permitido é de capacidade do processamento dos appliances dentro dos throughputs e quantidade de requisições solicitados.

2.8.24. Deve permitir autenticação dos usuários em bases remotas como, no mínimo, Microsoft Active Directory, RADIUS e OpenLDAP.

2.8.25. A interface gráfica de gerenciamento deve permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando.

2.8.26. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional.

2.8.27. A interface gráfica deve permitir a reinicialização do equipamento.

2.8.28. A Solução de gerenciamento deve possuir uma única console que permita a organização, gerenciamento, configuração e aplicação das políticas de segurança, regras de balanceamento, aceleração, cache em todos os equipamentos que compõem a solução de WAF com balanceamento.

2.8.29. A Gerência deve ter capacidade de obter e analisar eventos em tempo real

2.8.30. A Solução de gerenciamento deve fornecer as seguintes funcionalidades no seu ambiente gráfico:

a) Adição, alteração ou remoção de aplicações a serem protegidas pelo firewall de proteção a aplicações Web.

b) Adição, alteração ou remoção de regras de balanceamento, aceleração e cache;

c) Obter e analisar eventos em tempo real e gerar relatórios durante a avaliação do tráfego;

d) Permitir utilizar as informações obtidas para refinar as políticas de segurança a qual gerou o evento;

e) Permitir a criação de listas de acesso baseadas em endereços IP. Deve ser possível definir os endereços IP de origem das sessões.

2.8.31. Deve manter internamente múltiplos arquivos de configurações do sistema.

2.8.32. Deve permitir a exportação e importação de regras e políticas para um novo dispositivo de forma simples.

2.8.33. Deve permitir o armazenamento de sua configuração em memória não volátil, no caso de uma queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

2.8.34. Deve suportar rollback de configuração e imagem.

2.8.35. Deve possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, traceroute, ping e log de eventos.

2.8.36. O sistema operacional do dispositivo deve permitir a utilização da ferramenta tcpdump, ou similar de qualidade igual ou superior, para captura e monitoração de pacotes em quaisquer de suas interfaces de rede, permitindo que as capturas sejam armazenadas em formato libpcap.

2.8.37. A execução do tcpdump, ou ferramenta similar, não deve impactar no desempenho dos appliances. Permitir a definição de funcionalidades e dados requeridos por auditores.

2.8.38. O armazenamento dos primeiros 30 dias deve ser local.

2.8.39. O armazenamento dos demais dias poderá ser local ou remoto.

2.8.40. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog.

2.8.41. Possuir agente de gerenciamento SNMP, MIB SNMP II, extensões MIB SNMP, MIB bridging (RFC 1493), que possua descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem.

2.8.42. Suporte ao protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).

2.9. **Garantia:**

2.9.1. Os componentes da solução devem estar em linha de fabricação até a data de assinatura do contrato e a data de final de suporte (end-of-suport) deve ser após termino do contrato desta solução.

2.9.2. O serviço de garantia do fabricante contempla garantir o correto e pleno funcionamento de todos os itens adquiridos, seja software e os componentes necessários para o funcionamento da solução.

2.9.3. A CONTRATADA deverá garantir a substituição de qualquer módulo defeituoso de software ou componentes necessários para o funcionamento da solução durante o prazo contratado.

2.9.4. Não haverá custos adicionais para a CONTRATANTE de substituição de quaisquer componentes durante o período de garantia.

2.9.5. Prazo de garantia e suporte do fabricante deve ser de 01 (um) ano, com atendimento em horário comercial.

2.10. **Software e licenciamento:**

2.10.1. As assinaturas da solução de WAF devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo adicional por parte da CONTRATANTE na aquisição de novas licenças ou subscrições.

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

2.10.3. O licenciamento específico dos módulos de software WAF e Balanceamento de carga entre aplicações deve ser do tipo perpétuo, não sendo aceito modelo de subscrição. Demais módulos de software que compõem a solução podem ser por subscrição.

2.10.4. Deve estar incluso no fornecimento, o licenciamento de toda a solução do appliance virtual, com seus módulos de software, pelo período de 1 (um) ano, incluindo o suporte do fabricante em regime 8x5 de segunda a sexta-feira de 8:00h às 18:00h, exceto feriados .

ITEM 02 – Serviços técnicos especializados globais de instalação, configuração, ativação

2.11. Os serviços técnicos especializados previstos nesta contratação compreendem as atividades necessárias para implantação, configuração, ativação, migração e colocação em produção da nova solução de segurança de aplicações Web (WAF), garantindo sua adequada integração ao ambiente tecnológico atualmente existente no IPSM.

2.12. Os serviços deverão ser executados por profissionais especializados e certificados na solução ofertada, contemplando todas as etapas necessárias para disponibilização da solução em pleno funcionamento, incluindo parametrização, configuração de políticas de segurança, ativação de funcionalidades, testes operacionais, validações técnicas e apoio à equipe técnica do IPSM durante o processo de implantação e migração da solução atualmente existente.

2.13. Os serviços de instalação e configuração da solução serão executados no local definido pela CONTRATANTE, observando integralmente as características técnicas, requisitos e condições estabelecidos neste Termo de Referência, bem como as melhores práticas e recomendações dos fabricantes dos equipamentos e softwares envolvidos.

2.14. A CONTRATADA deverá fornecer todos os componentes, acessórios e cabos necessários à interligação física dos elementos da solução, bem como realizar a instalação, configuração e testes operacionais de todos os softwares contemplados na contratação.

2.15. A CONTRATADA deverá, ainda, realizar a migração das regras de WAF e Load Balance atualmente existentes no ambiente BIG-IP V13 do IPSM, assegurando a continuidade operacional do ambiente e a mínima interrupção dos serviços durante o processo de transição.

3. DETALHAMENTO DOS SERVIÇOS PREVISTOS NO OBJETO

3.1. **ITEM 1 - Solução integrada de segurança de Data Center WAF (WEB APPLICATION FIREWALL):**

3.1.1. A solução integrada de segurança de aplicações Web (WAF) deverá ser fornecida em appliance virtual compatível com o hypervisor AHV – Nutanix, contemplando licenciamento, subscrições, suporte técnico do fabricante e funcionalidades necessárias à proteção das aplicações institucionais do IPSM.

3.1.2. A solução deverá contemplar, no mínimo:

3.1.2.1. Balanceamento, cache e aceleração Web com capacidade mínima de 1 Gbps de inspeção de tráfego em camada 7;

3.1.2.2. Appliance virtual compatível com o hypervisor AHV - NUTANIX;

3.1.2.3. Proteção de aplicações Web (Web Application Firewall – WAF) com throughput mínimo de 1 Gbps;

3.1.2.4. Licenciamento de base de dados de reputação de IPs;

3.1.2.5. Licenciamento de base de dados voltada à proteção proativa contra ameaças conhecidas;

3.1.2.6. Suporte técnico do fabricante em regime 8x5, pelo período de 12 (doze) meses.

3.2. **ITEM 2 - Serviços técnicos especializados globais de instalação, configuração:**

3.2.1. Os serviços técnicos especializados compreendem as atividades necessárias para implantação, configuração, parametrização, ativação, migração e colocação em produção da solução integrada de segurança de aplicações Web (WAF) contemplada neste Termo de Referência.

3.2.2. Os serviços deverão ser executados em regime Turn-Key, abrangendo todas as etapas necessárias para disponibilização da solução em pleno funcionamento no ambiente tecnológico do IPSM.

3.2.3. A CONTRATADA deverá executar, no mínimo, as seguintes atividades:

3.2.3.1. Instalação, configuração e ativação da solução WAF e seus componentes de software;

3.2.3.2. Configuração de regras de WAF e balanceamento de carga das aplicações;

3.2.3.3. Instalação da máquina virtual (VM) do appliance WAF, incluindo configuração e ativação dos recursos de balanceamento de carga inerentes à solução;

3.2.3.4. Migração das regras de WAF F5 BIG IP VE existente no ambiente do IPSM;

3.2.3.5. Integração da solução com as aplicações existentes no ambiente institucional;

3.2.3.6. Realização de testes operacionais e validações de funcionalidade da solução implantada.

3.2.3.7. A CONTRATADA deverá executar todas as atividades com profissionais especializados e certificados na solução ofertada, assegurando a continuidade operacional do ambiente e a mínima interrupção dos serviços durante o processo de implantação e migração.

3.3. O serviço de Suporte Técnico a ser prestado pelo FABRICANTE deverá contemplar assistência continuada em regime 8x5 (oito horas por cinco dias da semana) à solução integrada de segurança de aplicações Web (WAF), abrangendo os serviços contratados, respectivas subscrições e licenças disponibilizadas, compreendendo atividades de sustentação, manutenção, atualização, diagnóstico, suporte operacional e resolução de incidentes, de forma a garantir a continuidade, disponibilidade, segurança e pleno funcionamento da solução implantada no ambiente tecnológico do IPSM.

3.4. O FABRICANTE deverá garantir a regularidade e a continuidade da prestação dos serviços de suporte técnico durante toda a vigência contratual.

3.5. Sempre que necessário, a CONTRATADA deverá acionar o suporte do fabricante da solução, sem prejuízo de sua responsabilidade pela efetiva resolução das demandas apresentadas pela CONTRATANTE.

3.6. O atendimento da CONTRATADA deverá garantir a continuidade da operação da solução de segurança de aplicações Web (WAF), minimizando riscos operacionais e assegurando a disponibilidade, integridade e segurança do ambiente tecnológico protegido.

3.7. Os serviços de Suporte Técnico compreendem todas as atividades necessárias ao adequado funcionamento da solução, incluindo diagnóstico e identificação de problemas, ajustes, parametrizações, apoio técnico na utilização da plataforma, correção de falhas, defeitos ou mal funcionamento dos recursos disponibilizados, aplicação de atualizações, correções de segurança e demais atividades necessárias à manutenção da estabilidade do ambiente.

3.8. Durante a vigência contratual, todas as atualizações, correções, melhorias e evoluções disponibilizadas pelo fabricante para os itens constantes neste Termo de Referência deverão estar incluídas no escopo da solução, sem custos adicionais à CONTRATANTE.

3.9. O Suporte Técnico será acionado por meio de um Sistema de Abertura de Chamado ou, na sua ausência, um canal direto de atendimento (email ou telefone). Esse contato deverá ser feito pela **Gerência e equipe de Infraestrutura/Redes** da **Assessoria de Tecnologia da Informação - ATI** da CONTRATANTE **.** Para solicitação de atendimentos de Suporte Técnico, a CONTRATANTE irá realizar contato por meio dos dispositivos supracitados informando, detalhadamente, qual é o problema e o nível de severidade.

3.10. O agendamento de data e horário das visitas para realização da manutenção corretiva deverá ser previamente acordado com a CONTRATANTE, por meio da formalização para os emails: tulio@ipsm.gov.br / geovani.lombardi@ipsm.gov.br / monica.santos@ipsm.gov.br.

3.11. O atendimento será acompanhado pela **Gerência e equipe de Infraestrutura/Redes** da **Assessoria de Tecnologia da Informação - ATI** da CONTRATANTE**.**

3.12. No caso da manutenção corretiva ocorrer de forma imediata à abertura do Chamado Técnico e não haver tempo para formalização do agendamento via email, o FABRICANTE e/a CONTRATADA poderá entrar em contato direto com a **Gerência e equipe de Infraestrutura/Redes** da **ATI** da CONTRATANTE, por meio do telefone **(31) 3269-2000/3269-2053** ou, ainda, pelo celular **(31) 99973-9598.**

3.13. O Suporte Técnico deverá ocorrer, conforme descrito abaixo:

3.13.1. Remoto ou

3.13.2. Presencial, se o FABRICANTE optar.

3.14. O atendimento deverá ser formalizado por meio de Relatório Técnico, que deverá conter, no mínimo:

- Data do atendimento;
- Modalidade do atendimento realizado (remoto ou presencial);
- Identificação do responsável pela abertura do chamado;
- Identificação do responsável pelo atendimento;
- Descrição detalhada do serviço executado.

3.15. O valor contratado deverá abranger todos os encargos relacionados à prestação do suporte técnico, incluindo mão de obra especializada, acionamento de suporte do fabricante, ferramentas necessárias e demais despesas operacionais eventualmente necessárias à execução do objeto.

3.16. Para apuração do tempo de atendimento e solução de problemas, os chamados são classificados em **04 (quatro) Níveis de Severidade**, de acordo com a tabela a seguir:

Severidade	Descrição / Escopo
1	Um problema que tenha um impacto crítico na capacidade da CONTRATANTE em manter sua infraestrutura ativa. Um número significativo de usuários do sistema e/ou da rede é incapaz de executar adequadamente as suas tarefas. O sistema e/ou a rede estão inoperantes ou severamente degradados.
2	Um problema que tenha um impacto na capacidade da CONTRATANTE em manter sua infraestrutura ativa, cuja severidade seja significativa, porém não crítica. O funcionamento do sistema ou da rede é afetado, e a operação é realizada de modo restrita
3	Um problema que não cause grande impacto na capacidade da CONTRATANTE em manter sua infraestrutura ativa. Geralmente a origem são problemas pontuais que envolvem poucos usuários.
4	Não é um problema e sim suporte para ajustes ou otimizações. Requisições de informações, melhorias ou esclarecimentos relativos às funcionalidades.

SEVERIDADE 1

Para os problemas classificados como de **Severidade 1**, o suporte técnico será prestado em regime 8x5 (oito horas por cinco dias da semana) com atendimento em até 2 (duas) horas corridas após o registro de chamado.

O problema deve ser contingenciado ou solucionado em até 4 (quatro) horas corridas após início do atendimento, ou a partir das respostas da CONTRATADA e/o FABRICANTE, quando solicitado. O tempo aguardando as respostas da CONTRATANTE não será contabilizado no tempo de atendimento.

SEVERIDADE 2

Para os problemas classificados como de **Severidade 2**, o suporte técnico será prestado em regime 8x5 (oito horas por cinco dias da semana) com atendimento em até 4 (quatro) horas corridas após o envio de registro do chamado.

O problema deve ser contingenciado ou solucionado em até 6 (seis) horas úteis após início do atendimento, ou a partir das respostas da CONTRATADA e/o FABRICANTE, quando solicitado. O tempo aguardando as respostas da CONTRATANTE não será contabilizado no tempo de atendimento.

SEVERIDADE 3

Para os problemas classificados como de **Severidade 3**, o suporte técnico será prestado em regime 8x5 (oito horas por cinco dias da semana) com atendimento em até 6 (seis) horas úteis após o envio de registro do chamado.

O problema deve ser contingenciado ou solucionado em até 8 (oito) horas úteis após início do atendimento, ou a partir das respostas da CONTRATADA e/o FABRICANTE, quando solicitado. O tempo aguardando as respostas da CONTRATANTE não será contabilizado no tempo de atendimento.

SEVERIDADE 4

Para os problemas classificados como de **Severidade 4**, o suporte técnico será prestado em regime 8x5 (oito horas por cinco dias da semana) com atendimento em até 8 (oito) horas úteis após o envio de registro do chamado.

O problema deve ser contingenciado ou solucionado em até 10 (dez) horas úteis após início do atendimento, ou a partir das respostas da CONTRATADA e/o FABRICANTE, quando solicitado. O tempo aguardando as respostas da CONTRATANTE não será contabilizado no tempo de atendimento.

4. FUNDAMENTAÇÃO DA CONTRATAÇÃO

A presente contratação tem por finalidade a modernização da infraestrutura de segurança do ambiente de Data Center do IPSM, por meio da aquisição de solução integrada de segurança de aplicações Web (WAF – Web Application Firewall), balanceamento de carga de aplicações e demais funcionalidades correlatas, contemplando também os serviços especializados de instalação, configuração, ativação e colocação em produção da solução.

Atualmente, o IPSM utiliza em seu ambiente tecnológico a plataforma BIG-IP Virtual Edition da fabricante F5 Networks, responsável pela proteção de aplicações web institucionais, balanceamento de carga entre servidores, inspeção de tráfego criptografado, proteção contra ameaças em camada de aplicação e garantia da disponibilidade dos serviços disponibilizados pelo Instituto. A referida solução desempenha papel estratégico e essencial na infraestrutura de tecnologia da informação do IPSM, atuando diretamente na proteção do ambiente de aplicações críticas, mitigação de vulnerabilidades, continuidade operacional dos sistemas institucionais e preservação da disponibilidade, integridade e confidencialidade das informações trafegadas.

Entretanto, conforme manifestação formal (139692356) da empresa responsável pela solução atualmente utilizada pelo IPSM, a versão BIG-IP Virtual Edition V16 entrou em processo de descontinuidade pelo fabricante, encontrando-se em condição de "End of Technical Support (EoTS)", situação que inviabiliza a continuidade da renovação contratual anteriormente existente. Nesse cenário, a permanência da solução atualmente implantada, sem suporte técnico oficial do fabricante, sem atualizações de segurança, sem correções de vulnerabilidades e sem garantia operacional, representa **elevado risco ao ambiente tecnológico do IPSM**, especialmente considerando tratar-se de solução diretamente relacionada à segurança de aplicações web e à proteção do ambiente de Data Center institucional.

A ausência de suporte oficial compromete a capacidade institucional de resposta a incidentes de segurança, a aplicação de correções críticas, a atualização de assinaturas de proteção, bem como a manutenção da estabilidade e disponibilidade dos serviços tecnológicos suportados pela plataforma.

Dessa forma, a presente contratação não se caracteriza como mera renovação contratual da solução anteriormente utilizada, mas sim como contratação de nova versão da plataforma tecnológica, contemplando modernização da infraestrutura de segurança atualmente existente, atualização tecnológica da solução WAF e adequação do ambiente do IPSM às atuais práticas e requisitos de segurança da informação e continuidade operacional.

A nova solução pretendida contempla funcionalidades avançadas de proteção de aplicações web, balanceamento inteligente de carga, proteção contra ameaças avançadas, mitigação de ataques automatizados, inteligência de ameaças, inspeção de tráfego criptografado, integração com ferramentas de monitoramento e correlação de eventos, mecanismos avançados de disponibilidade e recursos aderentes às melhores práticas modernas de cibersegurança.

Além disso, a contratação permitirá a continuidade segura da operação das aplicações institucionais do IPSM, assegurando suporte técnico especializado do fabricante, atualizações contínuas da plataforma, correções de segurança e evolução tecnológica compatível com as necessidades atuais do ambiente computacional do Instituto.

A contratação mostra-se, portanto, **indispensável** para garantir a continuidade operacional, a proteção da infraestrutura tecnológica institucional e a mitigação de riscos associados à utilização de solução descontinuada e sem suporte oficial do fabricante, preservando a segurança, disponibilidade e desempenho das aplicações críticas do IPSM.

5. REQUISITOS DA CONTRATAÇÃO

5.1. Da participação de consórcios:

5.1.1. Não será permitida a participação de empresas reunidas em consórcio, considerando a natureza da contratação pretendida e a necessidade de centralização da responsabilidade técnica e operacional da solução.

5.1.2. A presente contratação envolve o fornecimento, implantação, configuração, ativação, migração e suporte técnico especializado de solução integrada de segurança de aplicações Web (WAF) do fabricante F5 Networks, incluindo serviços relacionados à sustentação, atualização, suporte técnico especializado contínuo e administração da solução implantada no ambiente tecnológico do IPSM, os quais devem ser executados de forma coordenada, contínua e compatível, exigindo padronização de procedimentos, uniformidade operacional e gestão unificada da execução contratual.

5.1.3. A eventual participação de empresas em consórcio poderá acarretar dificuldades operacionais e gerenciais relacionadas à definição de responsabilidades, ao acionamento do suporte técnico, à gestão de incidentes, ao cumprimento dos níveis de serviço estabelecidos e à atuação tempestiva em situações que possam comprometer a disponibilidade, segurança e continuidade operacional da solução contratada.

5.1.4. A fragmentação de responsabilidades inerente à atuação consorciada poderá comprometer a eficiência da fiscalização contratual, dificultando o acompanhamento da execução, a apuração de responsabilidades e a adoção de medidas corretivas, em prejuízo da continuidade, disponibilidade, integridade e confiabilidade dos serviços relacionados à solução de segurança do IPSM.

5.1.5. Visando assegurar maior controle administrativo, uniformidade na execução contratual, mitigação de riscos operacionais e efetividade da fiscalização, fica vedada a participação de consórcios na presente contratação, nos termos do art. 15 da Lei Federal nº 14.133/2021.

5.2. Da Participação de cooperativas:

5.2.1. Não será permitida a participação de sociedades cooperativas na presente contratação, considerando a natureza técnica, especializada e continuada do objeto.

5.2.2. A execução contratual demanda prestação contínua e coordenada de serviços especializados relacionados à solução integrada de segurança de aplicações Web (WAF) do IPSM, incluindo atividades de implantação, configuração, ativação, migração, suporte técnico, sustentação, manutenção e atualização da solução, exigindo responsabilidade técnica centralizada, atuação padronizada e atendimento tempestivo às demandas da CONTRATANTE.

5.2.3. A prestação dos serviços envolve, ainda, a necessidade de disponibilidade operacional contínua, observância aos níveis de serviço estabelecidos, atuação especializada em ambiente crítico de segurança da informação e pronta resposta a incidentes que possam comprometer a disponibilidade, integridade, segurança e continuidade operacional do ambiente tecnológico do IPSM.

5.2.4. A eventual execução contratual por meio de sociedade cooperativa poderá comprometer a uniformidade operacional, a centralização da gestão técnica, a responsabilização direta pela execução dos serviços e a efetividade da fiscalização contratual, considerando as particularidades inerentes ao regime jurídico cooperativo.

5.2.5. Visando assegurar maior controle administrativo, continuidade operacional, uniformidade na prestação dos serviços, mitigação de riscos operacionais e efetividade da fiscalização contratual, fica vedada a participação de sociedades cooperativas na presente contratação.

5.2.6. A vedação encontra respaldo no art. 5º da Lei Federal nº 14.133/2021, que estabelece os princípios do planejamento, da eficiência e do interesse público nas contratações públicas. Assim, a exclusão de sociedades cooperativas tem como objetivo garantir a adequada execução do objeto, resguardando a continuidade dos serviços, a efetividade da fiscalização contratual e a adequada gestão do contrato.

5.3. Da Subcontratação:

5.3.1. Não será admitida a subcontratação do objeto contratual, considerando a necessidade de centralização da responsabilidade técnica e operacional da execução contratual.

5.3.2. A presente contratação envolve serviços especializados relacionados ao fornecimento, implantação, configuração, ativação, migração e suporte técnico especializado de solução integrada de segurança de aplicações Web (WAF), cuja execução demanda atuação coordenada, padronizada e contínua, especialmente em razão da criticidade da solução para o ambiente tecnológico do IPSM.

5.3.3. A eventual subcontratação poderá comprometer a efetividade da fiscalização contratual, dificultar a apuração de responsabilidades, impactar o cumprimento dos níveis de serviço estabelecidos e aumentar os riscos relacionados à continuidade operacional, disponibilidade, integridade e segurança da solução contratada.

5.4. Da Sustentabilidade:

5.4.1. Não serão exigidos critérios de sustentabilidade na presente contratação.

5.5. Da Indicação de Marcas ou Modelos:

5.5.1. A presente contratação contempla solução propriedade da fabricante F5 Networks, considerando a necessidade de compatibilidade técnica com o ambiente atualmente existente no IPSM, a integração com a infraestrutura tecnológica já implantada, a migração das regras e configurações atualmente utilizadas, bem como a continuidade operacional da solução de segurança de aplicações Web (WAF) utilizada pelo Instituto.

5.5.2. A indicação do fabricante decorre de necessidade técnica devidamente justificada, considerando a padronização do ambiente tecnológico, a compatibilidade entre os componentes da solução, a continuidade dos serviços atualmente prestados, a mitigação de riscos operacionais e a necessidade de manutenção da interoperabilidade com a infraestrutura existente no IPSM.

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

Não se aplica à presente contratação, uma vez que a indicação da solução do fabricante F5 Networks decorre de exigência técnica devidamente justificada, relacionada à necessidade de plena compatibilidade com o ambiente tecnológico já implantado no IPSM.

Atualmente, a infraestrutura de segurança da informação do Instituto encontra-se estruturada com soluções do referido fabricante, sendo a adoção de tecnologia diversa potencialmente geradora de incompatibilidades operacionais, aumento de complexidade na gestão, elevação de riscos de indisponibilidade e comprometimento da eficiência dos mecanismos de proteção existentes.

A utilização de solução do mesmo fabricante visa assegurar:

- a interoperabilidade nativa com os componentes já existentes;
- a manutenção da padronização tecnológica do ambiente;
- a continuidade operacional dos serviços de segurança;
- a otimização dos processos de administração, suporte e monitoramento;
- e a mitigação de riscos técnicos e operacionais decorrentes da heterogeneidade de soluções críticas.

Dessa forma, a indicação não configura direcionamento indevido, mas sim decisão técnica fundamentada, indispensável para garantir a integridade, a segurança e a continuidade dos serviços suportados pela infraestrutura de TI do IPSM.

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

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

5.8. **Da Garantia da Contratação:**

5.8.1. Será exigida a garantia da contratação, no percentual de **10% (dez por cento)** do valor inicial do contrato.

5.8.1.1. A fixação da garantia contratual no percentual de **10% (dez por cento)** justifica-se em razão da relevância, criticidade e complexidade dos serviços relacionados à solução integrada de segurança de aplicações Web (WAF) do IPSM, incluindo o fornecimento da solução, subscrições, suporte técnico especializado, implantação, configuração, ativação, migração e sustentação do ambiente tecnológico protegido pela plataforma.

5.8.1.2. Trata-se de contratação diretamente relacionada à segurança da informação, à continuidade operacional e à disponibilidade dos serviços tecnológicos institucionais do IPSM, considerando que a solução contratada desempenha funções essenciais de proteção de aplicações web, balanceamento de carga, mitigação de ameaças cibernéticas e manutenção da disponibilidade dos sistemas institucionais.

5.8.1.3. A exigência de garantia contratual em percentual superior ao mínimo legal mostra-se adequada e proporcional, tendo por finalidade resguardar a Administração quanto a eventuais prejuízos decorrentes do inadimplemento contratual, falhas na implantação da solução, indisponibilidade do ambiente protegido, descumprimento dos níveis de serviço estabelecidos ou falhas na prestação dos serviços de suporte técnico especializado.

5.8.1.4. A exigência de garantia contratual no percentual de **10% (dez por cento)** está amparada pelos artigos 96 e 98 da Lei Federal nº 14.133/2021, sendo compatível com a natureza continuada do objeto, os riscos envolvidos na execução contratual, a criticidade da solução e a relevância dos serviços prestados ao IPSM, sem configurar restrição indevida à competitividade do certame.

5.8.1.5. A garantia poderá ser apresentada nas modalidades: seguro-garantia, fiança bancária, caução em dinheiro ou títulos da dívida pública, título de capitalização.

5.8.1.6. O endosso da garantia será encaminhado, no prazo máximo de **30 (trinta) dias**, prorrogáveis por igual período, a critério da CONTRATANTE, contados da assinatura do contrato.

5.8.1.7. No caso de optar pela modalidade seguro-garantia, conforme disposto no § 3º do art. 96 da Lei Federal nº 14.133, de 2021, o prazo será **30 (trinta) dias** contado da data de homologação do procedimento e anterior à assinatura do contrato.

5.8.2. Caso utilizada a modalidade de seguro-garantia, a apólice deverá ter validade durante a vigência do contrato, permanecendo em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.

5.8.2.1. A garantia em dinheiro deverá ser efetuada em favor da CONTRATANTE, em conta específica, com correção monetária.

5.8.2.2. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia ou por aquele que o substituir em suas competências.

5.8.2.3. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

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

5.9.1. Além da garantia legal prevista no art. 26 da Lei Federal nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor – CDC), a CONTRATADA deverá assegurar a manutenção das condições de suporte, subscrição e garantia da solução ofertada durante toda a vigência contratual, conforme condições estabelecidas neste Termo de Referência.

5.9.1.1. As garantias legal e contratual não se sobrepõem, devendo os seus prazos ser somados.

5.9.2. A CONTRATADA deverá garantir, durante toda a vigência contratual, a manutenção ativa do suporte técnico e das garantias disponibilizadas pelo fabricante da solução ofertada, incluindo acesso às atualizações, correções, melhorias, assinaturas de segurança, bases de inteligência e demais recursos disponibilizados no âmbito das subscrições contratadas.

5.9.3. A garantia e o suporte do fabricante deverão permanecer válidos e ativos durante toda a execução contratual, sem qualquer ônus adicional à CONTRATANTE.

5.9.4. A garantia será prestada com vistas a manter a qualidade do serviço prestado, sem qualquer ônus ou custo adicional à CONTRATANTE.

5.9.5. Uma vez notificada, a CONTRATADA realizará a reparação dos serviços que apresentarem vício ou defeito no prazo de até **10 (dez) dias úteis**, contados a partir da data de recebimento da notificação.

5.9.6. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da CONTRATADA, aceita pela CONTRATANTE.

5.9.7. Decorrido o prazo para correção das falhas identificadas sem o atendimento da solicitação da CONTRATANTE ou a apresentação de justificativas pela CONTRATADA, fica a CONTRATANTE autorizada a contratar fornecedor diverso para executar os reparos, ajustes ou a substituição de componentes, bem como a exigir da CONTRATADA o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia do serviço prestado.

5.9.8. O custo referente ao reparo na prestação do serviço durante o período da garantia será de responsabilidade da CONTRATADA.

5.9.9. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

5.10. **Da Vistoria:**

5.10.1. A vistoria prévia do local de execução dos serviços poderá ser realizada pelos fornecedores interessados, visando proporcionar pleno conhecimento das condições e peculiaridades do ambiente tecnológico onde será implantada a solução objeto da presente contratação.

5.10.2. A vistoria poderá ser substituída por declaração formal do fornecedor, assinada por seu responsável técnico, de que possui pleno conhecimento das condições locais, características do ambiente e peculiaridades da contratação, assumindo integral responsabilidade pela elaboração de sua proposta e pela execução do objeto

5.10.3. A não realização da vistoria prévia não poderá ser utilizada futuramente como fundamento para alegações de desconhecimento das condições do ambiente, dificuldades técnicas, omissões ou solicitação de acréscimos contratuais relacionados às condições existentes no IPSM.

5.10.4. O fornecedor que desejar realizar visita técnica deverá agendar dia e horário específico, até 02 (dois) dias antes da abertura do procedimento de contratação, sendo vedada a visita de mais de um fornecedor no mesmo momento.

5.10.5. A vistoria será realizada nas seguintes condições:

5.10.5.1. A vistoria deverá ser agendada junto à **Gerência de Infraestrutura da Assessoria de Tecnologia da Informação – ATI** , por meio do telefone **(31) 3269-2000/3269-2053** ou, ainda, pelo celular **(31) 99973-9598**, podendo a visita ser acompanhada por colaborador designado pela CONTRATANTE, com a finalidade de dirimir dúvidas estritamente técnicas relacionadas ao objeto da contratação.

5.10.5.2. Na visita técnica serão respondidas apenas perguntas de caráter técnico, limitadas ao Termo de Referência, não sendo possível prestar esclarecimentos quanto ao objeto a ser licitado entre outros tópicos que não sejam técnicos, uma vez que estes esclarecimentos estão condicionados a serem requisitados apenas via Portal de Compras, com acesso de todos os interessados, para que não haja vantajosidade competitiva.

5.10.6. Alegações posteriores relacionadas com o desconhecimento de condições locais ou de projetos porventura disponibilizados, se for o caso, não serão consideradas para reclamações futuras, ou de forma a desobrigar a sua execução.

5.10.7. A empresa interessada, ao optar pela não realização da vistoria técnica e apresentar proposta no procedimento licitatório, assumirá integral responsabilidade pela execução do objeto contratado, incluindo todos os custos, encargos, tributos, transporte, materiais, recursos técnicos e demais ônus necessários à plena execução dos serviços previstos neste Termo de Referência.

6. DA EXECUÇÃO DO OBJETO

6.1. **Do prazo e das condições da prestação do serviço:**

6.1.1. A execução do objeto será caracterizada pelo fornecimento, implantação, configuração, ativação, migração, colocação em produção e suporte técnico especializada da solução integrada de segurança de aplicações Web (WAF) previstos no **TÓPICO 1** e detalhados no **TÓPICO 3** deste Termo de Referência.

6.1.2. A entrega, implantação, ativação, configuração, migração e quaisquer outras atividades técnicas necessárias à plena operacionalização da solução deverão ocorrer de **forma integrada**, não sendo admitida a disponibilização parcial desses serviços contratados.

6.1.3. A CONTRATADA deverá promover o agendamento da reunião de **kick-off** com a CONTRATANTE, respeitando a disponibilidade mútua de agenda e o alinhamento prévio de data e horário, no prazo máximo de até **5 (cinco) dias úteis** após a assinatura do contrato, com o objetivo de alinhar as etapas de execução, cronograma de implantação, procedimentos operacionais, fluxos de atendimento e demais aspectos necessários à execução contratual.

6.1.4. A execução do objeto deverá observar os seguintes prazos, contados a partir do envio da Nota de Empenho pela CONTRATANTE à CONTRATADA:

6.1.4.1. Disponibilização das licenças/subscrições e suporte técnico do FABRICANTE da solução WAF: **até 15 (quinze) dias corridos;**

6.1.4.2. Implantação, instalação, configuração, ativação e colocação em produção da solução: **até 15 (quinze) dias corridos.** Mesmo prazo de entrega das licenças visto a possibilidade iniciar a preparação do ambiente para a implementação da solução adquirida.

6.1.4.3. Migração das regras de WAF e Load Balance atualmente existentes no ambiente BIG-IP V13 do IPSM: **até 15 (quinze) dias corridos;**

6.1.4.4. Prestação de serviço de suporte técnico especializado, de forma contínua, em regime 8x5, **durante toda a vigência contratual**, conforme definido no **TÓPICO 3** deste Termo de Referência.

6.2. **Prazos para realização dos serviços:**

6.2.0.1. Os prazos para a prestação do serviço de suporte técnico especializado serão em conformidade aos **Níveis de Severidade** que estão relacionados no **TÓPICO 3** deste Termo de Referência.

6.3. **Do local e horário da prestação do serviço:**

6.3.1. Os serviços poderão ser executados de forma remota ou presencial, conforme a natureza da demanda e necessidade da CONTRATANTE.

6.3.2. Quando necessária a execução presencial dos serviços, estes deverão ser prestados nas dependências do IPSM, localizado na Rua Paraíba, nº 575 e nº 576, Bairro Savassi, Belo Horizonte/MG, ou em outro local previamente indicado pela CONTRATANTE.

6.4. **Dos materiais a serem disponibilizados:**

6.4.1. A CONTRATADA deverá disponibilizar todos os recursos, componentes, softwares, ferramentas, acessórios, licenças, subscrições e demais elementos necessários à plena execução do objeto previsto no **TÓPICO 1** deste Termo de Referência, sem ônus adicional à CONTRATANTE.

7. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

7.1. **Do Recebimento:**

7.1.1. Os serviços prestados serão recebidos, de **forma única**, **provisoriamente e definitivamente,** pela **Chefia da Assessoria de Tecnologia da Informação - ATI**, **com o apoio, acompanhamento e validação técnica da Gerência de Infraestrutura,** mediante **Ateste de Recebimento** quando verificado o cumprimento das exigências de caráter técnico e administrativo.

7.1.1.1. 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.

7.1.2. A CONTRATADA fica obrigada 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/Definitivo**.

7.1.3. O prazo para recebimento de **forma única**, **provisoriamente e definitivamente** deverá ocorrer no prazo **de até 10 (dez) dias após a entrega do serviço** e poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

7.1.4. 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.

7.1.5. 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 a CONTRATADA para emissão de nota fiscal no que diz respeito à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.1.6. O prazo para a solução, pela CONTRATADA, 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.

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

7.2. **Da Liquidação:**

7.2.1. A Liquidação será efetuada no prazo de até **10 (dez) dias** corridos contados da data do recebimento definitivo do serviço e respectivo aceite da CONTRATANTE.

7.2.2. 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:

7.2.2.1. O vencimento;

7.2.2.2. A data da emissão;

7.2.2.3. Os dados do contrato e do órgão Contratante;

7.2.2.4. O período respectivo de execução do objeto;

7.2.2.5. O valor a pagar; e

7.2.2.6. Eventual destaque do valor de retenções tributárias cabíveis.

7.2.3. 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 a CONTRATADA providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à CONTRATANTE.

7.2.4. 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.

7.2.5. A Liquidação também só ocorrerá após a apresentação e análise da seguinte documentação:

7.2.5.1. **Relatório Técnico** elaborado pela CONTRATADA com a descrição do serviços realizados, conforme detalhado no **TÓPICO 3** e no **item 3.14** deste Termo de Referência;

7.2.5.2. **Parecer Técnico**, também devidamente assinado pela CONTRATANTE, atestando a realização à contento dos serviços.

7.3. **Do Pagamento:**

7.3.1. 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 a CONTRATADA indicar e **no prazo de até 30 (trinta) dias corridos**, contados a partir da data final da liquidação a que se referir, com base nos documentos fiscais devidamente conferidos e aprovados pela CONTRATANTE.

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

7.3.2. No caso de atraso pela CONTRATANTE, por culpa exclusiva da Administração, os valores devidos à CONTRATADA serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, de acordo com a variação do Índice Nacional de Preços ao Consumidor Amplo (IPCA).

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

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

7.3.4. A CONTRATADA deve garantir a manutenção dos requisitos de habilitação previstos neste documento durante toda a contratação.

7.3.4.1. Eventuais situações de irregularidades fiscal ou trabalhista da CONTRATADA não impedem o pagamento, se o objeto tiver sido executado e atestado. Tal hipótese ensejará, entretanto, a adoção das providências tendentes ao sancionamento da CONTRATADA e rescisão contratual.

7.3.5. A CONTRATADA 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.

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

7.3.6.1. Não produzir os resultados acordados;

7.3.6.2. Deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

7.3.6.3. Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

8. PROCEDIMENTO DE TRANSIÇÃO E FINALIZAÇÃO DO CONTRATO

8.1. Não serão necessários procedimentos específicos de transição contratual, considerando as características do objeto e a natureza continuada da solução.

8.2. Entretanto, o contrato em questão deverá ter início em **25/06/2026**, em razão do término da vigência do contrato atualmente vigente e, ainda, da necessidade de continuidade da prestação dos serviços relacionados à solução de segurança de aplicações Web (WAF), de modo a evitar riscos operacionais, indisponibilidade dos serviços e impactos à segurança do ambiente tecnológico do IPSM.

9. GESTÃO DA CONTRATAÇÃO

9.1. **Regras Gerais:**

9.1.1. 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 Lei Federal nº 14.133, de 2021, e artigos 15 e 16 do Decreto 48.587, de 2023.

9.1.2. As comunicações entre a CONTRATANTE e a CONTRATADA devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

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

9.1.4. Após a assinatura do contrato, a CONTRATANTE poderá convocar o representante da empresa contratada para reunião inicial para 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 da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

9.1.5. 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.

9.1.6. 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.

9.1.7. A fiscalização e a gestão do contrato serão exercidas pela **Chefia da Assessoria de Tecnologia da Informação - ATI, com o apoio, acompanhamento e validação técnica da Gerência de Infraestrutura**.

9.2. **Da Fiscalização do Contrato:**

O **Decreto nº 48.587, de 17/03/2023 - Art. 2º** - estabelece as atribuições do **Fiscal** do contrato, a saber:

VI – fiscal do contrato: pessoa designada pela autoridade competente para realizar a fiscalização do cumprimento das disposições contratuais, tendo por parâmetro os resultados previstos, visando à qualidade da prestação e adotando providências necessárias ao fiel cumprimento do contrato.

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

9.2.2. 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 inciso II do art. 16 do Decreto nº 48.587, de 2023.

9.2.3. 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.

9.2.4. 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.

9.2.5. 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.

9.2.6. 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.

9.2.7. 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.

9.2.8. 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.

9.2.9. A fiscalização de que trata esta cláusula não exclui, nem reduz a responsabilidade da CONTRATADA 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.

9.3. **Da Gestão do Contrato:**

O **Decreto nº 48.587, de 17/03/2023 - Art. 2º** - estabelece as atribuições do **Gestor** do contrato, a saber:

V – gestor do contrato: pessoa designada pela autoridade competente para realizar o acompanhamento dos aspectos administrativos do contrato, tratando de questões relativas ao planejamento da execução da contratação, aspectos econômicos, prorrogações, além de promover as medidas necessárias à fiel execução das condições previstas no ato convocatório e no instrumento de contrato;

9.3.1. 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.

9.3.2. 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.

9.3.3. 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.

9.3.4. 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.

9.3.5. 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, repactuações ou rescisões contratuais, nos termos do inciso V, do art. 15 do Decreto nº 48.587, de 2023.

9.3.6. 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.

9.3.7. 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.

9.3.8. 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.

9.4. **Do Preposto:**

9.4.1. Não será necessária a designação de preposto pela CONTRATADA.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. 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.

10.1.1. Para a etapa competitiva do pregão eletrônico, será observado **intervalo mínimo de diferença entre lances**, aplicável tanto aos lances intermediários quanto ao lance que vise cobrir a melhor oferta, nos termos do art. 18 e do art. 57 da Lei nº 14.133/2021 e do Decreto Estadual nº 48.723/2023.

10.1.2. 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**.

10.1.3. 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$ 500,00 (quinhentos reais)**.

10.1.4. A metodologia adotada para o **Valor Absoluto Fixo** leva em consideração a proporcionalidade em relação ao valor estimado da contratação, a prevenção de lances inexequíveis ou irrisórios, a maior eficiência da disputa e a observância aos princípios da razoabilidade, competitividade e economicidade.

10.2. **Dos critérios de aceitabilidade da proposta:**

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

11. HABILITAÇÃO

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

11.1.1. **Habilitação Jurídica:**

11.1.1.1. 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;

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

11.1.1.3. 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;

11.1.1.4. 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;

11.1.1.5. 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;

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

11.1.1.7. 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;

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

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

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

11.1.2.2. 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.

11.1.2.3. 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 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.

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

11.1.2.5. Prova de inexistência de débitos inadimplidos perante a 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.

11.1.2.6. 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.

11.1.3. **Qualificação Econômico-Financeira:**

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

11.1.4. **Qualificação Técnico-Operacional e Técnico-Profissional:**

11.1.4.1. 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.

11.1.4.2. Para fins de habilitação e qualificação técnica, a licitante deverá apresentar:

11.1.4.3. Comprovação de aptidão para fornecimento, implantação, ativação e prestação de serviços técnicos especializados compatíveis com o objeto desta contratação, por meio de atestado(s), certidão(ões) ou declaração(ões) emitido(s) por pessoa jurídica de direito público ou privado, ou por documentos comprobatórios emitidos na forma do § 3º do art. 88 da Lei Federal nº 14.133, de 2021, demonstrando experiência compatível com as características técnicas, complexidade e natureza dos serviços previstos neste Termo de Referência, conforme §§ 2º e 5º do art. 67 da Lei Federal nº 14.133, de 2021.

I - Para comprovação da capacidade técnica exigida, será admitido o somatório de diferentes atestados, inclusive de períodos concomitantes, desde que compatíveis com as características técnicas, complexidade e natureza do objeto da contratação.

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 de 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 - A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, podendo ser solicitados pela Administração documentos complementares, tais como cópia do contrato que deu suporte à contratação, notas fiscais, ordens de fornecimento ou outros documentos correlatos.

11.1.4.4. Para fins de comprovação da capacidade técnica, a licitante deverá apresentar, no mínimo:

- 01 (um) atestado de capacidade técnica comprovando o fornecimento, implantação, ativação e prestação de serviços de suporte técnico em plataforma WAF (Firewall – NGFW) da fabricante F5 Networks.

11.1.4.5. A licitante deverá apresentar comprovação de que possui profissional tecnicamente certificado pelo fabricante da solução WAF (Firewall – NGFW) ofertada, apto à execução dos serviços de instalação, configuração, ativação e suporte técnico da solução.

11.1.4.6. O profissional certificado deverá possuir vínculo contratual ou empregatício com a licitante, devendo a comprovação correspondente ser apresentada juntamente à documentação de habilitação.

11.1.4.7. A licitante deverá apresentar comprovação de credenciamento, parceria ou autorização formal emitida pelo fabricante da solução WAF, habilitando-a à comercialização dos produtos e à execução dos serviços de instalação, implantação e suporte técnico relacionados à solução.

11.1.4.8. 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.

11.1.4.9. Poderão ser realizadas diligências junto às empresas ou órgãos declarantes a fim de confirmar e esclarecer as informações atestadas. Ainda, os atestados fornecidos poderão ser objeto de diligência para esclarecimento de quaisquer dúvidas quanto ao seu conteúdo, inclusive mediante solicitação dos respectivos contratos que lhes deram origem.

11.1.4.10. A licitante deverá possuir capacidade operacional para atendimento presencial no município de Belo Horizonte/MG e Região Metropolitana, quando necessário, observados os prazos estabelecidos nos níveis de severidade previstos neste Termo de Referência.

11.1.5. **Declaração:**

11.1.5.1. 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.

11.1.5.2. 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.

12. ALTERAÇÃO DE PREÇOS

12.1. Durante o prazo de vigência, os preços contratados poderão ser reajustados monetariamente com base no Índice Nacional de Preços ao Consumidor Amplo (IPCA), observado o interregno mínimo de 12 meses, contados do orçamento estimado, conforme disposto nos arts. 92, §§ 2ºe 3º da Lei nº 14.133/2021, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

12.2. Nos reajustes subsequentes ao primeiro, manter-se-á o marco inicial descrito no item 12.1.

12.3. Os preços são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado.

12.4. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

12.5. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, a CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

12.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

12.7. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

13. OBRIGAÇÕES ESPECÍFICAS DAS PARTES

13.1. **DA CONTRATANTE:**

13.1.1. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com o presente Termo de Referência, contrato e eventuais anexos.

13.1.2. Receber o objeto no prazo e condições estabelecidas neste documento.

13.1.3. Notificar a CONTRATADA, 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.

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

13.1.5. 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 da CONTRATADA.

13.1.6. Comunicar a CONTRATADA 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.

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

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

13.1.9. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA durante a execução do contrato ou documento que o substitua.

13.1.10. 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.

13.1.10.1. A Administração terá o prazo de até **30 (trinta) dias** corridos a contar da data do protocolo do requerimento, tratado no item 13.1.10, para decidir e admitir a prorrogação motivada por igual período, conforme art. 123, Lei Federal nº 14.133, de 2021.

13.1.11. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pela CONTRATADA no prazo máximo de 10 (dez) dias corridos.

13.1.12. Aplicar à CONTRATADA as sanções regulamentares.

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

13.1.14. Disponibilizar local adequado para a realização do serviço.

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

13.2. **DA CONTRATADA:**

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

13.2.2. 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.

13.2.3. Comunicar à 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.

13.2.4. 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.

13.2.5. 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.

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

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

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

13.2.9. Emitir faturas no valor pactuado, apresentando-as à CONTRATANTE para ateste e pagamento.

13.2.10. 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.

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

13.2.12. 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 à CONTRATANTE e não poderá onerar o objeto do contrato.

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

13.2.14. Paralisar, por determinação da 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.

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

13.2.16. 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.

13.2.16.1. 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

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

13.2.18. 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.

13.2.19. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da CONTRATANTE.

13.2.20. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas do contrato, 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.

13.2.21. 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 deste contrato.

13.2.22. 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.

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

13.2.24. 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.

13.2.25. Fornecer os relatórios técnicos atinentes à execução da prestação de serviço previsto no objeto deste Termo de Referência, mediante solicitação da CONTRATANTE e no prazo máximo de até 48 (quarenta e oito) horas da referida solicitação.

14. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

14.1. Comete infração administrativa, nos termos da Lei Federal nº 14.133, de 2021, a CONTRATADA que:

14.1.1. Der causa à inexecução parcial da contratação;

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

14.1.3. Der causa à inexecução total da contratação;

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

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

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

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

14.1.8. Apresentar documentação falsa ou prestar declaração falsa durante a contratação e execução do contrato;

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

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

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

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

14.2. Serão aplicadas à CONTRATADA que incorrer nas infrações acima descritas as seguintes sanções:

14.2.1. **Advertência** - quando a CONTRATADA 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;

14.2.2. **Impedimento de licitar e contratar** - quando praticadas as condutas descritas nos subitens 14.1.2 a 14.1.7, 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;

14.2.3. **Declaração de inidoneidade para licitar e contratar** - quando praticadas as condutas descritas nos subitens 14.1.8 a 14.1.12, bem como no subitem 14.2.2, que justifiquem a imposição de penalidade mais grave, conforme disposto no §5º, art. 156, da Lei Federal nº 14.133, de 2021);

14.2.4. **Multa:**

14.2.4.1. **0,5%** (cinco décimos por cento) por dia, até o trigésimo dia de atraso, sobre o valor do objeto não executado;

14.2.4.2. **20%** (vinte por cento) sobre o valor do fornecimento depois de ultrapassado o prazo de **30 (trinta) dias** de atraso, ou no caso de não entregado objeto, ou entrega com vícios ou defeitos ocultos que o torne impróprio ao uso a que é destinado, ou diminua-lhe o valor ou, ainda fora das especificações contratadas;

14.2.4.3. **2 %** (dois por cento) sobre o valor total do contrato ou instrumento equivalente, em caso de descumprimento das demais obrigações contratuais ou norma da legislação pertinente.

14.3. As sanções previstas nos subitens 14.2.1, 14.2.2 e 14.2.3 poderão ser aplicadas cumulativamente com a multa, conforme disposto no §7º, art. 156, da Lei Federal nº 14.133, de 2021.

14.4. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pela CONTRATANTE à CONTRATADA, 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.

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

14.6. 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;

14.7. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de **30 (trinta) dias**, a contar da data do recebimento da comunicação enviada pela autoridade competente.

14.8. 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.

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

14.9.1. A natureza e a gravidade da infração cometida;

14.9.2. As peculiaridades do caso concreto;

14.9.3. As circunstâncias agravantes ou atenuantes;

14.9.4. Os danos que dela provierem à CONTRATANTE;

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

14.10. 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 nesta última Lei citada, conforme art. 159 da referida Lei de Licitações.

14.11. 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.

14.12. A 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.

14.13. 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.

14.14. 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.

15. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

O custo estimado total da contratação é de **R$ 282.270,00** (duzentos e oitenta e dois mil e duzentos e setenta reais), conforme custos unitários apostos no quadro constante do **subitem 1.1** deste Termo de Referência.

16. ADEQUAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da presente contratação correrão por conta da dotação orçamentária do orçamento em vigor, aprovado pela Lei Orçamentária Anual n° 25.698, de 2026, de 14/01/2026.

A contratação será atendida pelas seguintes dotações:

2121 10 122 705 **2 017** 0001 **3 3** 90 **4002** 0 **49** 1;

2121 09 122 705 **2 018** 0001 **3 3** 90 **4002** 0 **49** 1;

2121 10 122 705 **2 017** 0001 **3 3** 90 **4002** 0 **60** 1;
2121 09 122 705 **2 018** 0001 **3 3** 90 **4002** 0 **60** 1.

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

Belo Horizonte, 14 de Maio de 2026.

_____

Nome do Elaborador: Mônica Cristina dos Santos
Chefe da Assessoria de Tecnologia da Informação
Masp: 1440390-1

Nome do Elaborador: Luiza de Santana Silva Xavier
Assistente Técnico de Seguridade Social
Masp: 1432014-7

Nome do Elaborador: Marco Túlio Gontijo
Gerente de Redes
Matrícula: 2855-0

_____

Nome do Aprovador: Cel QOR PM Evair dos Santos Oliveira
Diretor de Planejamento, Gestão e Finanças
Masp: 1594253-5

Documento assinado eletronicamente por **Monica Cristina dos Santos**, **Servidor(a) Público(a)**, em 15/05/2026, às 14:10, 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 **Marco Túlio Silva Gontijo**, **Prestador(a) de Serviços**, em 15/05/2026, às 14:47, 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 **Luiza de Santana Silva Xavier**, **Servidor(a) Público(a)**, em 15/05/2026, às 14:59, 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 **Evair dos Santos Oliveira**, **Diretor (a)**, em 15/05/2026, às 16:24, 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 **138669245** e o código CRC **3A692783**.

Referência: Processo nº 2120.01.0020876/2026-82 SEI nº 138669245