Tribunal de Justiça Militar do Estado de Minas Gerais

TERMO DE REFERÊNCIA

OBJETO: AQUISIÇÃO DE PRODUTOS E SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO:

LOTE 1: Renovação da solução de Firewall de Rede de Próxima Geração com suporte, licença, e garantia, incluindo comissionamento da solução - **produto Fortigate** da empresa Fortinet, com prazos e condições descritas neste Termo de Referência;

CATMAS: 09200070

ITEM	CÓDIGO	DESCRIÇÃO	QUANTIDADE
01	FG-200F-BDL-950-36	Renovação da solução de Firewall de Rede de Próxima Geração(NGFW), incluindo suporte e assinaturas de segurança por 36 meses.	02
02	-	Comissionamento da solução	02

1. INTRODUÇÃO

Este termo de referência tem por objetivo caracterizar os objetos a serem contratados; estabelecer normas, especificações e procedimentos que orientem a execução dos serviços e fornecimento dos materiais; estabelecer nível de qualidade desejado para os materiais e serviços com base nos elementos que constituem a contratação; estabelecer os critérios de medição e pagamento para os serviços que serão desenvolvidos durante o cumprimento e execução de cada objeto descrito em seu respectivo lote.

Todos os serviços e produtos que compõem o lote se caracterizam como comuns, de natureza contínua, apresentando padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado, conforme a seguir discriminadas.

2. SETOR REQUISITANTE

Diretoria de Tecnologia da Informação e Comunicação, com aprovação do CGTIC/TJMMG (Comitê de Gestão e Governança em Tecnologia da Informação e Comunicação do Tribunal de Justiça Militar de Minas Gerais) conforme Resolução n. 175/2016 do Tribunal de Justiça Militar do Estado de Minas Gerais.

3. BREVE HISTÓRICO E JUSTIFICATIVA

Em 2017, o Tribunal de Justiça Militar de Minas Gerais aderiu ata da UFSJ através do processo SEI 17.0.000001096-0 que contemplou a compra de duas unidades da solução Firewall de Rede de Próxima Geração Fortigate 300D da fabricante Fortinet. Essa aquisição representou um importante salto para a segurança de rede da instituição pois a solução anterior permitia apenas a execução de regras básicas de roteamento. Dentre os ganhos que foram proporcionados podemos citar filtros de navegação WEB granulares, integração com o LDAP Active Directory, balanceamento de carga entre links de Internet, QoS de saída de internet(priorizando banda para realização de vídeo-audiências), VPN para acesso remoto/teletrabalho seguro, IPS (detecção e prevenção de intrusão) etc. Concomitante ao appliance, a adesão incluiu o software de análise de logs FortiAnalyzer, pelo qual é possível extrair relatórios de utilização da rede com bastante detalhamento, tornando o estudo de utilização de rede e averiguação de incidentes de segurança bastante facilitado.

De acordo com o site da fabricante, o modelo 300D atingirá fim de vida útil(End of Life) em Outubro do presente ano. Sendo assim após esse período, não é possível extender a garantia e suporte do equipamento, bem como subscrições de segurança fornecidas pelo fabricante. Logo, é necessário a renovação da solução tecnológica, tratando a como ativo crítico para que as funções de prestação de serviço do TJMMG permaneçam em atividade.

O período de 36 meses se faz necessário para possibilitar que este serviço crítico e essencial para continuidade do negócio seja prestado de maneira continuada. As possíveis interrupções contratuais causadas por eventual falta de interesse da CONTRATADA na renovação contratual, geralmente causadas por dificuldades na manutenção dos preços em virtude de elevação da cotação do dólar, e a necessidade de se fazer novas licitações em curto prazo de tempo, elevam sobremaneira o risco de interrupção contratual e de falta de suporte da solução. Tais fatores aumentam o risco de indisponibilidade de serviços críticos de TI indispensáveis para o próprio funcionamento do órgão. Por outro lado, um período superior ao especificado estaria sujeito a risco de obsolescência tecnológica e de mercado.

A demanda faz parte dos investimentos em manutenção, atualização dos softwares e equipamentos que sustentam os sistemas administrativos e judiciais utilizados na Justiça Militar. Dada a dependência cada vez maior dos meios eletrônicos para a realização das atividades da Justiça Militar, faz-se necessária a constante modernização e reciclagem dos ativos de TI presentes no Tribunal para que as obrigações não sejam prejudicadas por intercorrências ou gargalos. Ademais, dado o crescimento recente de ameaças cibernéticas ao setor público e privado, faz-se necessária a constante atualização dos ativos de TI como parte de estratégia de mitigação dos riscos.

Diante desse cenário, justifica-se a necessidade e seus quantitativos que serão devidamente detalhados neste Termo de Referência, seguramente alinhado com os estudos de viabilidade da presente aquisição, esclarecendo que estes quantitativos são os mínimos necessários para o atendimento da demanda.

Trata-se de solução fundamental e imprescindível para a segurança da rede do TJMMG, tendo em vista o expressivo aumento de ataques cibernéticos a orgãos governamentais com objetivo de comprometer a infraestrutura tecnológica e os sistemas disponibilizados. O surgimento diário de novas ameaças e a crescente complexidade desses ataques aumenta a

dificuldade de detecção, análise e resposta em tempo hábil. Essa situação pode ocasionar vazamentos de dados sigilosos e comprometer a disponibilidade de sistemas críticos hospedados no TJMMG.

A segurança das informações e a segurança de todo parque computacional do TJMMG depende das funcionalidades de firewall, filtro de aplicações, filtro WEB, controle de tráfego e antivírus executadas por essa solução. Por tratar-se do principal elemento de segurança aplicado ao ambiente deste Tribunal, seu pleno funcionamento é essencial para a implementação das políticas de segurança definidas por este Tribunal.

Dentre as funcionalidades exercidas pela solução de segurança, podemos citar os filtros de pacotes, que restringem o trafego baseado no endereço IP de origem ou destino, ou, através das portas utilizadas pelos serviços. Mais especializados, os filtros de estado e sessão utilizam uma característica do principal protocolo de transporte utilizado, o Transmission Control Protocol (TCP), que é sua tabela de estados de conexão.

Já o filtro de conteúdo é capaz de permitir ou negar acessos baseado em categorização ou em palavras-chaves definidas em uma lista. O filtro de aplicação possibilita o bloqueio de aplicações como Facebook, Youtube, Netflix, entre outros, de forma dinâmica e baseada em atributos, incluindo categorias, subcategorias e tecnologia.

As funções de intrusão e detecção de intrusão, Intrusion prevention system (IPS) e Intrusion detection system (IDS), analisam o trafego prevenindo atividades potencialmente maliciosas por meio de assinaturas ou comportamento conhecidos. A funcionalidade de inspeção SSL permite a verificação de trafego de rede criptografados, o que proporciona um nível maior de segurança ao ambiente. Por fim, a funcionalidade de QoS (Quality of Service) permite definir limites de utilização de recursos baseados em serviços ou usuários e a VPN possibilita o acesso remoto seguro aos usuários em regime de telebralho e a Fábrica de Software.

Todas as funções citadas acima estão relacionadas com a proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um usuário ou instituição contra ameaças que podem paralisar, desgovernar, comprometer e até mesmo inutilizar sistemas críticos disponibilizados pelo TJMMG, internamente ou extenamente tais como Eproc, SEI, Consultas Processuais, Codex, entre outros, caso esses ataques consigam ultrapassar as camadas de segurança hoje existentes.

Essas ameaças vêm, cada vez mais, tornando-se grandes riscos para as atividades desenvolvidas pelo TJMMG, podendo tornar os sistemas computacionais indisponíveis e colocando em risco a confiabilidade e a integridade dos dados nele armazenados.

4 . DESCRIÇÃO DO OBJETO - ITEM 1

1.Características do appliance e performance

1.1.Throughput de, no mínimo, 27 Gbps para pacotes UTP de 1518 e 512 bytes.
1.2.Suporte a, no mínimo, 3M conexões TCP simultâneas
1.3.Suporte a, no mínimo, 280K novas conexões por segundo

1.4.Throughput de, no mínimo, 13 Gbps de VPN IPSec
1.5.Estar licenciado para ou suportar sem o uso de licença, 2,5K túneis de VPN IPSEC Site-to-Site simultâneos
1.6.Estar licenciado para ou suportar sem o uso de licença, 16K túneis de clientes VPN IPSEC simultâneos
1.7.Throughput de, no mínimo, 2 Gbps de VPN SSL
1.8.Suporte a 500 clientes de VPN SSL simultâneos
1.9.Suportar no mínimo 5 Gbps de throughput de IPS
1.10. Suportar no mínimo 4 Gbps de throughput de Inspeção SSL
1.11. Throughput de, no mínimo, 3 Gbps com as seguintes funcionalidade habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
1.12. Possuir ao menos 16 interfaces 1Gbps
1.13. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance

2. Requisitos Mínimos de Funcionalidade
2.1.A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
2.2.Deverá ser do mesmo fabricante dos itens “SOFTWARE DE GERENCIAMENTO” e “SOFTWARE DE RELATÓRIOS”, para garantir total compatibilidade;
2.3. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
2.4.As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
2.5. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
2.6. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
2.7. O software deverá ser fornecido em sua versão mais atualizada;
2.8. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
2.9. O gerenciamento da solução deve suportar a interface de administração via web no próprio dispositivo de proteção de rede
2.10. Os dispositivos de proteção de rede devem possuir suporte a 1024 VLAN Tags 802.1q;
2.11. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 8023ad e LACP;
2.12. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
2.13. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM ePIM-DM);
2.14. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
2.15. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
2.16. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
2.17. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet lógicas
2.18. Deve suportar NAT dinâmico (Many-to-1);
2.19. Deve suportar NAT dinâmico (Many-to-Many);
2.20. Deve suportar NAT estático (1-to-1);

2.21. Deve suportar NAT estático (Many-to-Many);
2.22. Deve suportar NAT estático bidirecional 1-to-1;
2.23. Deve suportar Tradução de porta (PAT);
2.24. Deve suportar NAT de Origem;
2.25. Deve suportar NAT de Destino;
2.26. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
2.27. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
2.28. Deve suportar NAT64 e NAT46;
2.29. Deve implementar o protocolo ECMP;
2.30. Deve implementar balanceamento de link por hash do IP de origem;
2.31. Deve implementar balanceamento de link por hash do IP de origem e destino;
2.32. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quatro links;
2.33. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede
2.34. Enviar log para sistemas de monitoração externos, simultaneamente;
2.35. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
2.36. Proteção anti-spoofing;
2.37. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
2.38. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
2.39. Suportar OSPF graceful restart;
2.40. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
2.41. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
2.42. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
2.43. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
2.44. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
2.45. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;
2.46. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;
2.47. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;
2.48. A configuração em alta disponibilidade deve sincronizar: Sessões;
2.49. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
2.50. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
2.51. A configuração em alta disponibilidade deve sincronizar:Tabelas FIB;
2.52. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

2.53. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
2.54. A utilização dos dispositivos em alta disponibilidade não deve impor limitações quanto à utilização de sistemas virtuais (contextos);
2.55. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
2.56. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;
2.57. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolação das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos)
2.58. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
2.59. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, o licenciamento do dispositivo de segurança não pode ter nenhuma relação com sua configuração de rede como, mas não limitado a, configuração de interfaces, endereços lógicos, etc , podendo ser utilizado por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

3. Controle por Política de Firewall
3.1.Deverá suportar controles por zona de segurança
3.2.Controles de políticas por porta e protocolo
3.3.Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações
3.4.Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança
3.5.Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS)
3.6.Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound)
3.7.Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
3.8.Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
3.9.Controle de inspeção e de-criptografia de SSH por política;
3.10. Suporte a objetos e regras IPV6;
3.11. Suporte a objetos e regras multicast;
3.12. Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
3.13. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

4. Controle de Aplicações
4.1.Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer

aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
4.2.Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos
4.3.Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede,voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
4.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel,facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;
4.5.Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo
4.6.Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
4.7.Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor
4.8.Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
4.9.Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex
4.10. Identificar o uso de táticas evasivas via comunicações criptografadas;
4.11. Atualizar a base de assinaturas de aplicações automaticamente;
4.12. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
4.13. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
4.14. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
4.16. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
4.17. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
4.18. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MSSQL, IMAP, DNS, LDAP, RTSP e SSL
4.19. O fabricante deve permitir a solicitação de inclusão de aplicações na base de

assinaturas de aplicações;
4.20. Deve alertar o usuário quando uma aplicação for bloqueada;
4.21. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
4.22. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc) possuindo granularidade de controle/políticas para os mesmos;
4.23. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
4.24. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
4.25. Deve possibilitar a diferenciação de aplicações Proxies (psiphon3, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
4.26. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
4.27. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client- Server, Browse Based, Network Protocol, etc)
4.28. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação
4.29. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Categoria da aplicação
4.30. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Aplicações que usem técnicas evasivas, utilizadas por malwares como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos, etc;

5. Prevenção de Ameaças
5.1.Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante
5.2.Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
5.3.As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
5.4.Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
5.5.Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Antipyware e Antivirus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
5.6.As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
5.7.Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
5.8.Exceções por IP de origem ou de destino devem ser possíveis nas regras e assinatura a assinatura;
5.9.Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens

5.10. Deve permitir o bloqueio de vulnerabilidades
5.11. Deve permitir o bloqueio de exploits conhecidos
5.12. Deve incluir proteção contra ataques de negação de serviços
5.13. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de padrões de estado de conexões;
5.14. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;
5.15. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;
5.16. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise heurística;
5.17. Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;
5.18. Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;
5.19. Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados
5.20. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
5.21. Detectar e bloquear a origem de portscans;
5.22. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
5.23. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
5.24. Possuir assinaturas para bloqueio de ataques de buffer overflow;
5.25. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
5.26. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e antispyware, permitindo a criação de exceções com granularidade nas configurações;
5.27. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
5.28. Identificar e bloquear comunicação com botnets;
5.29. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
5.30. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e controle de aplicação;
5.31. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos
5.32. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
5.33. Os eventos devem identificar o país de onde partiu a ameaça;
5.34. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms
5.35. Proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos
5.36. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança

6. Filtro de URL

6.1.Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
6.2.Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
6.3.Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
6.4.Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
6.5.Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
6.6.Possuir pelo menos 60 categorias de URLs;
6.7.Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
6.8.Permitir a customização de página de bloqueio;
6.9.Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);

7.Identificação de Usuários

7.1.Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
7.2.Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
7.3.Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;
7.4.Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
7.5.Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
7.6.Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

7.7.Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
7.8.Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
7.9.Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução
7.10. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator

8. QoS e Traffic Shaping

8.1.Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
8.2.Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
8.3.Suportar a criação de políticas de QoS e Traffic Shaping por porta;
8.4.O QoS deve possibilitar a definição de classes por Banda Garantida;
8.5.O QoS deve possibilitar a definição de classes por Banda Máxima;
8.6.O QoS deve possibilitar a definição de classes por Fila de Prioridade
8.7.Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
8.8.Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

9.Filtro de Dados
9.1.Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
9.2.Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
9.3.Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

10. Geo Localização
10.1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;
10.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
10.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

11. VPN
11.1. Suportar VPN Site-to-Site e Cliente-To-Site;
11.2. Suportar IPSec VPN;
11.3. Suportar SSL VPN;
11.4. A VPN IPSEc deve suportar 3DES;
11.5. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
11.6. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
11.7. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
11.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
11.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI
11.10. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
11.11. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6
11.12. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
11.13. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
11.14. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
11.15. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
11.16. Atribuição de DNS nos clientes remotos de VPN;

11.17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
11.18. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
11.19. Suportar leitura e verificação de CRL (certificate revocation list);
11.20. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
11.21. O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SCCM, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
11.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação;
11.23. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação;
11.24. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário;
11.25. Deverá manter uma conexão segura com o portal durante a sessão;
11.26. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

12. Condições operacionais
12.1. Alimentação / tensão de 100-240 VAC
12.2. Possuir conector para fonte de alimentação redundante;
12.3. Alimentação / frequência de 50/60 Hz
12.4. Temperatura - faixa de operação de 0º a 40º C
13. Suporte técnico e licenciamento
13.1. Suporte técnico do fabricante na modalidade **durante 36 meses;**
13.2. Todas as funcionalidades de segurança que necessitem de atualização deverão estar licenciadas para 36 meses;
13.3. Durante a vigência do suporte técnico deverá estar inclusa atualização de software sem nenhum custo adicional;
13.4. A prestação do suporte técnico não poderá haver limites no quantitativo de abertura de chamados;
13.5. Os chamados deverão ser abertos através de portal WEB;
13.6. Na apresentação da proposta comercial a proponente deverá fornecer declaração do fabricante dos produtos ofertados, declarando que a proponente possui credenciamento do mesmo para realizar a comercialização e configuração de suas soluções. Tal declaração se faz necessária devido a alta criticidade da solução pois em caso de falha ou imperícia o CONTRATANTE poderá interromper acesso a todos os serviços de TI ou ficar vulnerável a ataques que indisponibilizariam todo o ambiente tecnológico.

4.1 - DESCRIÇÃO DO OBJETO - ITEM 2

14.1. O comissionamento deverá ser realizado presencialmente no edifício sede do Tribunal de Justiça Militar de Minas Gerais em Belo Horizonte. Todo o trabalho de instalação física e conexões de cabos serão realizadas pela equipe da CONTRATADA sob acompanhamento dos técnicos da contratante.

A execução dos serviços técnicos especializados deverá ser realizada por profissional certificado pelo fabricante da solução, sendo indispensável apresentação de documentação original do fabricante que comprove a validade da certificação quando solicitada pela CONTRATANTE a qualquer momento.

Esta etapa envolve a instalação, configuração e migração para o novo appliance em substituição ao atual em funcionamento, a saber, Fortigate 300D, mantendo todas as configurações atuais e promovendo melhorias devido a atualização tecnológica da solução descrita. Dentre as configurações atuais, citamos:

14.1.2 Configurações básicas de conectividade
14.1.3 Registro e ativação de licenças Atualização de software
14.1.4 Configuração de zonas de segurança, VLANs e roteamento interno
14.1.5 Configurações dos serviços de segurança como IPS e Anti-Malware
14.1.6 Configuração de balanceamento de carga de links WAN
14.1.7 Configuração de VPN
14.1.8 Configuração de regras de aplicação
14.1.9 Integração com base LDAP ou Radius
14.1.10 Configuração de autenticação SSO
14.1.11 Configuração de filtro de conteúdo por grupo de usuários
14.1.12 Configuração da unidade de alta disponibilidade
14.1.13 Configuração de QoS por serviços e/ou aplicações
14.1.14 Configuração de modo HA - Alta disponibilidade entre os appliances

5. DA ENTREGA:

5.1) Todos os equipamentos fornecidos e seus componentes serão novos, de primeiro uso e deverão estar acondicionados adequadamente em caixa lacrada de fábrica, de forma a propiciar completa segurança durante o transporte;

5.2) O prazo para entrega dos equipamentos será de **45 (quarenta e cinco) dias corridos**, contados da notificação pelo TRIBUNAL.

6. DOS QUESITOS MÍNIMOS DAS PROPOSTAS

6.1 - Para fins de comprovação da QUALIFICAÇÃO TÉCNICA dos produtos, a proponente deve apresentar em sua proposta, documentação ou referências que evidenciem a marca, o modelo e o fabricante, podendo apresentar os CATÁLOGOS e descritivos técnicos, de maneira a explicitar as reais características dos produtos e que todas elas atendam às especificações técnicas contidas neste Termo de Referência;

6.2 - A proposta apresentada deverá conter o CNPJ da proponente, prazo de validade e ser endereçada ao Tribunal de Justiça Militar do Estado de Minas Gerais – TJMMG;

6.3 - Nos preços da proposta deverão estar inclusas todas as despesas e custos diretos e indiretos, como impostos, taxas e fretes. Os valores deverão ser expressos em algarismos arábicos, na moeda Real, considerados apenas até os centavos;

6.4 - A proposta deverá conter marca e modelo do objeto a ser fornecido, podendo apresentar catálogos, folders, manuais e/ou outros documentos que comprovem que o ofertado atende às características técnicas mínimas deste Termo de Referência;

6.5 - As proponentes preferencialmente deverão apresentar preços unitários e totais, conforme modelo oferecido nos quadros abaixo e obedecendo às demais exigências do Edital do certame:

ITEM	CÓDIGO	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
01	FG-200F-BDL-950-36	Renovação da solução de Firewall de Rede de Próxima Geração(NGFW), incluindo suporte e assinaturas de segurança por 36 meses.	02		
02	-	Comissionamento da solução	02		

7. MODALIDADE E TIPO DE LICITAÇÃO

7.1. A contratação será em pregão eletrônico de lote único, como forma de assegurar o alinhamento e coerência em termos de qualidade técnica, indispensáveis devido a criticidade da solução para a CONTRATANTE.

8. OBRIGAÇÕES ESPECÍFICAS DAS PARTES

8.1. DA CONTRATADA

1 - Fornecer os produtos nas quantidades, prazos e condições pactuadas, de acordo com as exigências constantes neste documento;

2 - Emitir faturas no valor pactuado, apresentando-as ao CONTRATANTE para ateste e pagamento;

3 - Atender prontamente as orientações e exigências inerentes à execução do objeto contratado;

4 - Reparar, remover, refazer ou substituir, às suas expensas, no todo ou em parte, os itens em que se verificarem defeitos ou incorreções resultantes da execução do objeto, no prazo máximo de 3 dias úteis;

5 - Assegurar ao CONTRATANTE o direito de sustar, recusar, mandar desfazer ou refazer qualquer serviço/produto que não esteja de acordo com as normas e especificações técnicas estabelecidas neste Termo de Referência;

6 - Assumir inteira responsabilidade pela entrega dos materiais, responsabilizando-se pelo transporte, acondicionamento e descarregamento dos materiais;

7 - Responsabilizar-se pela garantia dos materiais empregados nos itens solicitados, dentro dos padrões adequados de qualidade, segurança, durabilidade e desempenho, conforme previsto na legislação em vigor e na forma exigida neste Termo de Referência;

8 - Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do objeto deste Termo de Referência;

9 - Não transferir para o CONTRATANTE a responsabilidade pelo pagamento dos encargos

estabelecidos no item anterior, quando houver inadimplência da CONTRATADA, nem onerar o objeto deste Termo de Referência;

10 Manter, durante toda a execução do objeto, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

11 - Quando for o caso, manter preposto, aceito pela Administração, para representá-lo na execução do objeto contratado;

12 - Responder pelos danos causados diretamente ao CONTRATANTE ou aos seus bens, ou ainda a terceiros, decorrentes de sua culpa ou dolo na execução do objeto.

13 - Comunicar à Administração, 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;

8.2. DO CONTRATANTE

1 - Acompanhar e fiscalizar os serviços, atestar nas notas fiscais/faturas o efetivo fornecimento do objeto deste Termo de Referência;

2 - Rejeitar, no todo ou em parte os itens entregues, se estiverem em desacordo com a especificação ou com a proposta de preços da CONTRATADA;

3 - Comunicar à CONTRATADA todas as irregularidades observadas durante o recebimento dos itens solicitados;

4 - Notificar a CONTRATADA no caso de irregularidades encontradas na entrega dos itens solicitados;

5 - Solicitar o reparo, a correção, a remoção ou a substituição dos materiais/serviços em que se verificarem vícios, defeitos ou incorreções;

6 - Conceder prazo de 03 (três) dias úteis, após a notificação, para a CONTRATADA regularizar as falhas observadas;

7 - Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

8 - Aplicar à CONTRATADA as sanções regulamentares;

9 - Exigir o cumprimento dos recolhimentos tributários, trabalhistas e previdenciários através dos documentos pertinentes;

10 - Disponibilizar local adequado para a realização do serviço, quando for o caso.

11 - Efetuar o pagamento no prazo previsto.

9. SANÇÕES ADMINISTRATIVAS

9.1. A licitante que deixar de entregar documentação exigida para o certame, apresentar documentação falsa, ensejar o retardamento da execução do objeto do certame, não mantiver a proposta, falhar ou fraudar a execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal ficará impedido de licitar e contratar com a Administração Pública do Estado de Minas Gerais e, se for o caso, será descredenciado do Cadastro Geral de Fornecedores do Estado de Minas Gerais, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas no edital e no contrato e das demais cominações legais.

9.2. A licitante/adjudicatária que cometer qualquer das infrações previstas na Lei Federal nº

8.666, de 21 de junho de 1993, na Lei Federal nº 10.520, de 17 de julho de 2002 e no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012, ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

1 - advertência por escrito;

2 - Multa de até 20% (vinte por cento) sobre o valor estimado do(s) lote(s) dos quais o licitante tenha participado e cometido a infração, ficando estabelecidos os seguintes percentuais:

2.1 - 0,3% (zero vírgula três por cento) por dia de atraso na execução do objeto, ou por dia de atraso no cumprimento de obrigação contratual ou legal, até o 30º (trigésimo) dia, calculados sobre o valor deste Contrato, por ocorrência;

2.2 - 10% (dez por cento) sobre o valor do Contrato, no caso de atraso superior a 30 (trinta) dias na execução do objeto ou no cumprimento de obrigação contratual ou legal, no caso de prestação do serviço em desacordo com as especificações contratadas ou em caso de inexecução parcial, com a possível rescisão contratual;

2.3 - 20% (vinte por cento) sobre o valor do contrato, na hipótese de a CONTRATADA, injustificadamente, desistir do Contrato ou dar causa à sua rescisão, bem como nos demais casos de descumprimento contratual, quando o TRIBUNAL, em face da menor gravidade do fato e mediante motivação da autoridade superior, poderá reduzir o percentual da multa a ser aplicada.

3 - Suspensão do direito de participar de licitações e impedimento de contratar com a Administração, pelo prazo de até 2 (dois) anos;

3.1 - Impedimento de licitar e contratar com a Administração Pública Estadual, nos termos do art. 7º da Lei Federal nº 10.520, de 17 de julho de 2002;

3.2 - Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

9.3. A sanção de multa poderá ser aplicada cumulativamente às demais sanções previstas no item 8.2, alínea 3.

9.4. A multa será descontada da garantia do contrato, quando houver, e/ou de pagamentos eventualmente devidos ao INFRATOR e/ou cobrada administrativa e/ou judicialmente.

9.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012, bem como o disposto na Lei Federal nº 8.666, de 21 de junho de 1993, Lei Estadual nº 14.184, de 31 de janeiro de 2002 e Portaria n. 1.157/19 do TJMMG.

9.6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

1 - Não serão aplicadas sanções administrativas na ocorrência de casos fortuitos, força maior ou razões de interesse público, devidamente comprovados.

9.7. A aplicação de sanções administrativas não reduz nem isenta a obrigação da CONTRATADA de indenizar integralmente eventuais danos causados a Administração ou a terceiros, que poderão ser apurados no mesmo processo administrativo sancionatório.

9.8. O pagamento da multa aplicada não exime a CONTRATADA da responsabilidade pelo cumprimento das obrigações a ela impostas por força do contrato.

9.9. As sanções relacionadas nos itens 9.3.1 e 9.3.2 serão obrigatoriamente registradas no

Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual - CAFIMP.

9.10. As sanções de suspensão do direito de participar em licitações e impedimento de licitar e contratar com a Administração Pública poderão ser também aplicadas àqueles que:

1 - Retardarem a execução do objeto;

2 - Comportarem-se de modo inidôneo;

2.1 - Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances;

3 - Apresentarem documentação falsa ou cometerem fraude fiscal.

9.11. Durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei Federal nº 12.846, de 1º de agosto de 2013, e pelo Decreto Estadual nº 46.782, de 23 de junho de 2015, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas ao Tribunal de Justiça do Estado de Minas Gerais, nos termos da Resolução n. 199/2018 - TJMMG, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

ANEXO DO TERMO DE REFERÊNCIA

ANEXO I

MODELO DE ATESTADO DE CAPACIDADE TÉCNICA

Atestamos, para os fins que se fizerem necessários, que o (a) Entidade/Empresa _____, inscrita no Cadastro Nacional de Pessoa Jurídica–CNPJ, sob o n.º: _____, prestou para esta Entidade ou Empresa os produtos/serviços ....., (**descrever neste espaço os serviços/produtos observando o disposto no escopo deste edital**), tendo tais produtos/serviços sido prestados no(s) período(s) de _____.

Atestamos, ainda, que os compromissos assumidos foram cumpridos satisfatoriamente, nada constando em nossos registros, até a presente data, que o(a) desabone comercialmente ou tecnicamente.

_____ (LOCAL), _____ DE _____ DE _____

_____

ASSINATURA E CARIMBO
(REPRESENTANTE LEGAL DA EMPRESA)

Documento assinado eletronicamente por **WILLIAM MARCONDES DE FREITAS SANTOS**, **Analista Judiciário/Administrador de Redes**, em 19/09/2023, às 09:09, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **OTALINO GERALDINO SOARES JUNIOR**, **Analista Judiciário**, em 19/09/2023, às 12:58, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JOANA EMÍLIA ROSA MEIRA**, **Assistente Judiciária**, em 19/09/2023, às 13:53, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://www.tjmmg.jus.br/servicos informando o código verificador **0278059** e o código CRC **270953CE**.

Rua Tomaz Gonzaga, 686 - Bairro de Lourdes
CEP 30180-143 - Belo Horizonte - MG