Coordenadoria de Informática
Setor de Autarquias Sul - Quadra 01 - Bloco L, Edifício CFA, Brasília/DF, CEP 70070-932
Telefone: (61) 3218-1830 - www.cfa.org.br

TERMO DE REFERÊNCIA Nº 16/2019/CFA

PROCESSO Nº 476900.001317/2019-88

Este Termo de Referência foi elaborado em cumprimento ao disposto no inciso incisos I e II, do artigo 8º e inciso II do artigo 21 do Decreto 3.555/00 e inciso I e § 2º do artigo 9º do Decreto nº 5.450/05. Apresento a seguir estudos preliminares realizados contendo elementos capazes de propiciar a avaliação do custo pela Administração, considerando o preço atualmente praticado, a definição de métodos, a estratégia de suprimento e o prazo de execução do contrato, quando for o caso.

1. DO OBJETO

Aquisição de solução de segurança de rede composta por um ou mais appliances, compreendendo equipamentos, software, treinamento e prestação de serviços com 03 (três) anos de garantia e suporte de software e hardware para atender ao Conselho Federal de Administração.

2. DA JUSTIFICATIVA

O Conselho Federal de Administração – CFA, buscando a constante melhoria e a celeridade no cumprimento de seu papel está modernizando a infraestrutura física e tecnológica. A ação concentra os investimentos em ativos destinados a aumentar a robustez do ambiente operacional do Conselho, elevando os níveis de performance e de tolerâncias a falhas e ataques cibernéticos.

Uma solução de segurança de rede para enfrentar os desafios e ameaças trazidos pelos ciberataques e usuários maliciosos, é imprescindível.

A atual ferramenta de segurança de rede (aker firewall) está obsoleta, fora de garantia, sem suporte, não atende mais as novas politicas de segurança e ataques cibernéticos mais sofisticados.

Desta forma faz-se necessário a aquisição de uma nova solução de segurança que atenda o Conselho e as futuras demandas do SEI - Sistema Eletrônico de Informação que tendem a aumentar significativamente com a entrada dos demais regionais localizados em todos os estados da federação .

3. DAS INFORMAÇÕES PRELIMINARES

3.1. Tecnologia Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui inspeção profunda de pacotes para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação; administração de largura de banda (QoS); VPN IPsec e SSL; IPS; prevenção contra ameaças de vírus e outros malware; filtro de URL; inspeção de tráfego criptografado; proteção de firewall de aplicação Web; proteção de vazamento de informações; e console remota de gerenciamento centralizado.

3.2. O equipamento deve ser novo e de primeiro uso. Todos os itens desse Termo de Referência devem estar em linha de produção e sendo comercializados pelo Fabricante;

3.3. Nenhum hardware e software fornecido poderá constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

3.4. Todos os itens deste Termo de Referência devem vir com a última versão de software e/ou firmware disponível pelo Fabricante no momento da aquisição;

3.5. Todos os itens deste Termo de Referência devem ser do mesmo fabricante;

3.6. Todos os equipamentos devem vir acompanhados de manuais (em português ou inglês) em mídia eletrônica;

3.7. O equipamento deverá ser fornecido de acordo com as características técnicas mínimas presentes neste projeto básico;

3.8. O fornecedor deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CFA ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros;

3.9. A solução entregue deverá ser completamente compatível com os serviços e dispositivos utilizados pelo Conselho, com os quais sua operação estará relacionada, facultando-se à Licitante a realização de vistoria prévia.

3.10. A solução deverá estar licenciada para quantidade ilimitada de usuários e também de endereços IP.

3.11. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico, como exemplo bare-metal.

3.12. A solução deverá contemplar a totalidade das capacidades exigidas, sendo permitido o uso de mais de um appliance para complementar a solução, caso o fabricante não possua todas as funções em um único equipamento.

3.13. Por appliance que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.

4. DAS ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

Especificações Técnicas Gerais:

4.1. A solução deve consistir de um ou mais equipamentos de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência, monitoramento e logs, sendo funcionalidades de NGFW reconhecimento de aplicações, prevenção de ameaças, DLP, proteção contra ameaças day zero, identificação de usuários e controle granular de permissões.

4.2. As funcionalidades de proteção de rede que compõem a plataforma de segurança podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

4.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

4.4. Uma interface completa de comando de linha (CLI command-line-interface) deverá ser acessível através da interface gráfica ou via porta serial.

4.5. A atualização de software deverá enviar avisos de atualização automáticos.

4.6. Além das funcionalidades de NGFW, o firewall deverá permitir a definição de redes, serviços, hosts, períodos de tempos, usuários e grupos, clientes e servidores.

4.7. O backup e o restabelecimento de configuração deverão ser feitos localmente, sendo possível sua transmissão por FTP ou e-mail com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

4.8. As notificações de monitoramento deverão ser realizadas via e-mail e SNMP.

O Firewall deverá ainda:

4.9. Suportar SNMP (v1, v2 e v3) e Netflow;

4.10. Possuir capacidade de inspeção profunda de pacotes;

4.11. Permitir estabelecer políticas de conversão de endereços (NAT) customizáveis para cada regra;

4.12. Possuir proteção contra flood, com mecanismos contra DoS (Denial of Service), DdoS (Distributed DoS) e bloqueio de portscan;

4.13. Possuir proteção contra anti-spoofing;

4.14. Possuir suporte a IPv4 e IPv6;

4.15. Em IPv6, suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969;

4.16. Suportar roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIMSM e IGMP);

4.17. Possuir balanceamento de link WAN que permita múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso;

4.18. Permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;

4.19. Implementar os serviços de DNS, Dynamic DNS, DHCP e NTP, de forma que o

Firewall seja o provedor destes serviços para a rede;

4.20. Possuir funcionalidade de qualidade de serviço do tipo traffic shapping (QoS) baseada em rede ou usuário;

4.21. Permitir estabelecimento de cotas cíclicas ou não-cíclicas, por usuários, para upload/download e pelo tráfego total;

4.22. Possuir otimização em tempo real de tráfego VoIP (voz sobre IP);e

4.23. Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

Especificações mínimas de desempenho do Firewall:

4.24. Performance mínima de 25 Gbps de throughput para todas as funções do firewall.

4.25. Performance mínima de 4,0 Gbps de throughput de IPS.

4.26. Performance mínima de 2,5 Gbps de throughput para controle de Antivírus/proxy.

4.27. Performance mínima de 2,5 Gbps de throughput de VPN.

4.28. Teto mínimo de conexões concorrentes (serviços DPI desabilitados): 4.000.000 (quatro milhões).

4.29. Suporte a, no mínimo, 60.000 (sessenta mil) novas conexões por segundo.

4.30. Suporte a, no mínimo, 500 túneis IPsec VPN.

4.31. Possuir número irrestrito de usuários licenciados.

4.32. Possuir unidade de armazenamento de, no mínimo, 60 GB para quarentena local, logs e relatórios.

4.33. A unidade de armazenamento pode ser interna ou externa.

4.34. Possuir no mínimo 8GB de memória RAM.

4.35. Possuir no mínimo 6 (seis) interfaces de rede 1000Base-TX.

4.36. Possuir no mínimo 6 (seis) portas SFP+ 10Gb, podendo ser fornecidos em módulo de expansão.

4.37. Possuir 1 (uma) interface do tipo console ou similar.

4.38. Possuir 1 (uma) fonte 100-240 VAC.

4.39. Possuir 1 (uma) fonte redundante 100-240 VAC.

Das políticas de controle que o firewall deve possuir:

4.40. Suporte a controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.

4.41. Monitoramento das políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.

4.42. Controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas (rede interna, DMZ, rede externa), redes e por tipos de serviços.

4.43. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

4.44. Controle de políticas por países via localização por IP.

4.45. Suporte a objetos e regras IPV6.

4.46. Suporte a objetos e regras multicast.

Da prevenção de Ameaças que o firewall deve prover:

4.47. Módulos de IPS, Antivírus, Anti-Malware e Firewall de Proteção Web (WAF), integrados em um ou em múltiplos appliances. Seja em um ou mais appliances, todos os requisitos deste termo de referência devem ser atendidos.

4.48. Identificação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.

4.49. Inspeção profunda de pacotes, com inclusão de assinaturas para prevenção de intrusão (IPS).

4.50. Customização de assinaturas de prevenção de intrusão (IPS).

4.51. Configuração de exceções por usuário, grupo de usuários, IP de origem ou de destino nas regras;

4.52. Configuração de maneira granular as políticas de IPS, Antivírus e Anti-Malware, possibilitando a criação de diferentes politicas por endereço de origem, endereço de destino, serviço ou a combinação de todos esses itens, com customização completa;

4.53. A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-emails.

4.54. A proteção Anti-Malware deverá possuir capacidade de realizar a proteção com emulação JavaScript.

4.55. Proteção em tempo real contra novas ameaças criadas.

4.56. Bloqueio de vulnerabilidades.

4.57. Bloqueio de exploits conhecidos.

4.58. Detecção e bloqueio do tráfego de rede que busque acesso a contact command e servidores de controle utilizando múltiplas camadas de DNS, AFC e firewall.

4.59. Proteção contra ataques de negação de serviços.

4.60. Imunidade contra ataques básicos tais como: SYN flood, ICMP flood, UDP Flood.

4.61. Bloqueio de arquivos por tipo.

4.62. Registro, na console de monitoramento, das 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.

4.63. Identificação, na ocorrência de eventos, do país de onde partiu a ameaça.

4.64. Configuração de diferentes políticas de controle de ameaças e ataques cujas políticas de segurança, considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino ou zonas de segurança.

Da prevenção de Aplicações Web (WAF), o firewall deve prover:

4.65. Para proteção do ambiente contra ataques, a solução deve possuir o módulo de Firewall de Aplicação Web (WAF - Web Application Firewall) integrado no próprio appliance de Firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

4.66. Deve realizar a inspeção profunda de pacotes (DPI deep packet inspection).

4.67. O firewall de aplicação Web (WAF) deverá ter a função de reverse proxy, com a função de URL hardening realizando deep-linking e prevenção dos ataques de path traversal ou directory traversal.

4.68. O firewall de aplicação Web (WAF) deverá realizar cookie signing com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor.

4.69. Proteção pelo menos contra os seguintes ataques, mas não limitado a: SQL injection, Cross-site scripting, directory traversal, entre outros.

4.70. A solução de firewall de aplicação Web (WAF) deve permitir definir endereços externos (virtual webservers) que devem ser traduzidos para endereços internos utilizando regras de DNAT (Destination NAT).

4.71. A solução de WAF deve permitir a visualização dos logs específicos para esta função em modo gráfico e em arquivo via comando de linha.

4.72. A solução de WAF deverá proteger o servidor web contra manipulação de cookies, fazendo que o web server ao definir um cookie tenha adicionado um segundo cookie no primeiro cookie contendo um hash a partir do primeiro cookie gerado, um valor e um segredo. Este segredo deverá ser conhecido apenas pelo WAF, fazendo com que uma requisição que não forneça um correto par de cookies seja identificada como manipulada e sendo assim dropada.

4.73. A solução de WAF deverá prover o hardening da URL contra reescrita. Quando um cliente requisitar um website todas as URLs do website serão assinaladas. Caso uma requisição não for assinalada ela deverá ser negada, evitando assim a manipulação da URL.

4.74. A solução de WAF deve conter a proteção dos servidores web contra vírus. Deverá permitir também selecionar se esta proteção será somente nos downloads, uploads e também em ambos sentidos, configurando o limite de tamanho dos arquivos a serem escaneados. A opção de escaneamento ilimitado também deverá estar presente na solução, sendo realizada o escaneamento de todos os arquivos sem limitações.

4.75. Deverá ser fornecida na solução de WAF o bloqueio de cliente por má reputação, baseados em localização geográfica (GeoIPClosed) e por RBL (Realtime Blackhole Lists).

4.76. A solução deverá realizar bloqueios de: violação de protocolos, anomalias de protocolos, requests (definindo limites), uso de opções de HTTP raramente utilizadas, robots, ataques genéricos, SQL Injection, XSS, tentativas de path traversal, trojans e de mensagens de outbound (mensagens de erro, por exemplo).

4.77. A solução de WAF deve permitir a utilização de autenticação direta na solução em vez de deixar a autenticação como responsabilidade do web server, utilizando autenticação básica em HTTP (usuário e senha) sem a geração de sessão de cookie bem como sem um logout dedicado e também permitir a autenticação via formulário com a geração de sessão de cookies e um logout dedicado é possível.

Da prevenção contra spams (antispam) que o firewall deve prover:

4.78. A solução de antispam deve permitir ser configurada, no mínimo, para os protocolos SMTP, SMTPS, POP, POPS, IMAP e IMAPS.

4.79. A solução de antispam deve permitir o bloqueio de ameaças de zero-hora e de ataques envolvendo spam, botnets, phishing, spyware entre outros.

4.80. Deve ser permitida a criação de políticas de permissão ou negação de tráfego de email de e para o servidor de email interno.

4.81. Todo o tráfego de email deve ter proteção de spam, malware, dados e arquivos.

4.82. A solução deve permitir a configuração de um limite de tamanho de email a ser escaneado, além de especificar as ações que devem ser tomadas no caso de um vírus ser detectado.

4.83. O bloqueio de emails indesejados deve ser baseado tanto para recepção quanto para o envio, permitindo o bloqueio de certos tipos de arquivos.

4.84. A solução de antispam deverá suportar, pelo menos, o modo de full email MTA (Mail Transfer Agent) e de proxy transparente.

4.85. No modo MTA a solução deverá receber e direcionar emails para seus específicos destinos, trabalhando com múltiplos domínios de emails e aplicando também proteções distintas para cada um destes domínios de emails. Deverá ser feito o armazenamento de emails quando servidores de email estiverem indisponíveis.

4.86. Todos os emails processados pela solução deverão gerar logs para consulta operacional ou de auditorias que se fizerem necessárias.

4.87. As políticas de SMTP devem ser configuradas no modo MTA para proteção de múltiplos domínios no servidor de email interno, protegendo o servidor de ataques remotos, realizando o escaneamento de vírus, a criptografia do email e os serviços de filtragem de emails.

4.88. A solução deverá possuir políticas em SMTP para o escaneamento de malware, permitindo que sejam tomadas ações em caso de detecção de um email contendo um vírus ou contento um anexo protegido. As definições das ações devem ser definidas em regras e ter, pelo menos, as seguintes possibilidades para estes emails detectados com vírus ou anexo protegido: entregues na forma que foram recebidas; descartados; limpos e então entregues; ou os emails devem ser colocados em quarentena.

4.89. Para o escaneamento do malware deverá permitir a configuração de notificações para os administradores, emissores e recipientes dos emails.

4.90. Diferentes políticas de escaneamentos devem ser configuradas para diferentes emissores e receptores.

4.91. A solução de antispam deve possuir um repositório automático de quarentena de emails.

4.92. Os atributos de spam em SMTP, SMTPS, POP3, POP3S, IMAP e IMAPS devem utilizar filtros de conteúdo e listas em tempo real (RBL – Realtime Blackhole Lists) indicando a lista de IPs que recusam a parar a proliferação de spam, sendo o responsável por um spam ou por retransmiti-los. Na detecção de um IP presente em uma RBL, o administrador deverá ter na solução a possibilidade de criar uma política definindo qual ação deverá ser realizada quando da identificação deste caso.

4.93. A solução deverá ser capaz de monitorar e restringir a transferência de arquivos contento dados sensíveis, incluindo a linha do assunto do email, o corpo da mensagem e os anexos para informações sensíveis ou confidenciais. Baseados em políticas a solução deve criptografar este email sensível ou confidencial, bem como deve ser rejeitado e enviado de acordo com as definições de politicas a serem configuradas na solução.

4.94. Para a identificação de dados sensíveis a solução deverá prover uma lista de definições para a identificação de tipos de dados financeiros e pessoais, como: número de cartões de crédito, números de seguridade social, endereços postais e endereços de emails.

4.95. As mensagens de emails e os anexos que forem criptografados deverão gerar um documento PDF que deve ser encriptado com uma senha. Esta senha pode ser definida pelo emitente do email, gerada pelo servidor para o recipiente e também ser gerada uma senha OTP (One time password) para o recipiente.

4.96. A quarentena de emails deverá identificar todos os bloqueios ocorridos solicitados na solução (RBL, dados sensíveis, vírus, tamanho de emails acima do limite de escaneamento, spams, entre outros). Os usuários deverão receber uma notificação de quarentena de acordo com a frequência determinada pelo administrador e

também devem acessar um portal de usuário para a visualização dos emails em quarentena, devendo tomar ações de acordo com as configurações permitidas pelos administradores.

4.97. A solução deve conter a proteção contra ataques de negação de serviços SMTP, especificando o número máximo de conexões, número máximo de conexões por host, número máximo de emails por conexão, número máximo de recipientes por email, a taxa de emails por minuto por host e a taxa de conexões por segundo por host.

Do controle e proteção de aplicações que o firewall deve prover:

4.98. Capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado.

4.99. Reconhecimento de, pelo menos, 1.500 (mil e quinhentas) aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de software.

4.100. Habilitação do escaneamento de micro app via console gráfica (GUI) e também via comando de linha (CLI).

4.101. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

4.102. Atualização automática da base de assinaturas de aplicações.

4.103. Reconhecimento de aplicações em IPv6.

4.104. Capacidade de limitar a banda usada por aplicações (traffic shaping).

4.105. Capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Integração ao LDAP poderá ser feita com instalação de agente.

4.106. Capacidade de 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.

4.107. Capacidade de permissão de uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

Do controle e da proteção para aplicações WEB que o firewall deve prover:

4.108. Especificação de política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou aplicada em uma única vez.

4.109. Capacidade de criação de políticas por usuários, grupos de usuários, IPs e redes;

4.110. Capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Radius, E-directory e base de dados local;

4.111. Apresentação, em todos os logs de URL, das informações dos usuários, conforme descrito na integração com serviços de diretório;

4.112. Definição de, pelo menos, 50 categorias de URLs;

4.113. Capacidade de criação de políticas baseadas em URL e Categoria de URL;

4.114. Capacidade de forçar o uso da opção “Safe Search” em sites de busca;

4.115. Capacidade de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante; independentemente do método de classificação, a categorização não deve causar atraso na comunicação ao usuário;

4.116. Suporte à criação de categorias personalizadas de URLs;

4.117. Suporte a bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

4.118. Customização de página de bloqueio;

4.119. Suporte à inclusão, nos logs do produto, de informações das atividades dos usuários;

4.120. Gravação, nos logs, das informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.

4.121. Filtragem por mime-type, extensão e tipos de conteúdos ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

Identificação de Usuários

4.122. Capacidade de criação de políticas baseadas na visibilidade e controle de quem (usuário) está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, Active Directory, Radius e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

4.123. 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).

4.124. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

4.125. Deve permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64 bits.

4.126. Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory.

Qualidade de Serviço (QoS)

4.127. Para controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, é exigido que o firewall, além da capacidade de permitir ou negar esses tipos de aplicações, deverá também ter a capacidade de controlá-las por políticas de largura de banda máxima, quando forem solicitadas por diferentes usuários ou aplicações.

4.128. A solução deverá suportar Traffic Shaping (QoS) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

4.129. Deverá possibilitar a configuração de limite e garantia de upload/download, bem como priorização do tráfego total e bit-rate de modo individual ou compartilhado.

4.130. Suportar priorização de tempo real (Real-Time) de protocolos de voz (VoIP).

Redes Privadas Virtuais (VPN)

4.131. Suportar VPN Site-to-Site e Client-to-Site.

4.132. Suportar IPsec VPN.

4.133. Suportar SSL VPN.

4.134. Suportar L2TP e PPTP.

4.135. Suportar acesso remoto SSL, IPSec e VPN Client para Android e iOS.

4.136. Deve ser disponibilizado o acesso remoto, limitado apenas pela capacidade de túneis VPN que o equipamento suporta, sem a necessidade de aquisição/aplicação de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL para estações Windows.

4.137. Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows e Linux.

4.138. Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, HTTP, HTTPS, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.

4.139. A VPN IPsec deve suportar: DES e 3DES, Autenticação MD5 e SHA-1;Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (Advanced Encryption Standard); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).

4.140. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Dell SonicWALL, Fortinet, Huawei, Juniper, Sophos e Palo Alto Networks.

4.141. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Malware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

4.142. Suportar autenticação via AD/LDAP, Token e base de usuários local;

4.143. Permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, Active Directory, Radius, eDirectory e via base de dados local;

Gerência Administrativa Centralizada

4.144. Possuir solução de gerenciamento centralizado, em uma única console, com administração de privilégios e funções, segregando, apropriadamente, as tarefas administrativas.

4.145. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

4.146. Estar licenciada para gerenciar as soluções de firewall de próxima geração.

4.147. Devem ser fornecidas soluções virtuais ou via appliances desde que obedeçam a todos os requisitos desta especificação.

4.148. Centralizar a gerência de todas as políticas e configurações do firewall sem necessidade de acesso direto aos equipamentos.

4.149. Deve permitir a criação de Templates para configurações.

4.150. Deve possuir indicadores do estado de equipamentos e rede;

4.151. Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.

4.152. Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.

4.153. Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc);

4.154. Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll-back de configurações para mudanças indesejadas;

4.155. Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos (trilha de auditoria).

4.156. Deve possuir integração com solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.

Gerência de Logs e Relatórios

4.157. Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.

4.158. Devem ser fornecidas soluções virtuais, softwares ou via appliances, desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 120GB de dados ou que permitam armazenar essas informações em unidades de armazenamento externas, conforme previsto nas especificações.

4.159. Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente de qual rede ou IP o usuário esteja se conectando.

4.160. Deve fornecer relatórios históricos para análises de mudanças ou comportamentos.

4.161. Deve conter customizações dos relatórios para inserção de logotipos próprios.

4.162. Deve permitir a exportação via PDF ou Excel.

4.163. Deve fornecer logs em tempo real, de auditoria e arquivados.

4.164. Deve possuir mecanismo de procura de logs arquivados.

4.165. Deve ter acesso baseado em Web com controles administrativos distintos.

5. DA INSTALAÇÃO E CONFIGURAÇÃO

5.1. Os valores referentes a instalação e configuração devem ser inclusos nos valores apresentados para solução;

5.2. A instalação e a configuração deverão ser realizados por técnicos prepostos pela Contratada, nas instalações do CFA;

5.3. A Contratada terá um prazo máximo de 60 (sessenta) dias corridos a partir da assinatura do contrato, para concluir a instalação e a configuração da solução, que serão demandados pela Conselho, findo o qual se aplicarão as penalidades contratuais cabíveis;

5.4. O CFA se reserva o direito de acompanhar e fiscalizar os serviços realizados pela Contratada verificando a aderência as especificações técnicas definidas, zelando pelo cumprimento de prazos e monitorando a qualidade dos serviços;

5.5. **A Contratada deverá apresentar, previamente à execução dos serviços de instalação, um plano de execução no prazo máximo de 10 (dez) dias da assinatura do contrato, detalhando fases e prazos estimados**;

5.6. O contratante aprovará o plano de execução no prazo máximo de 3 dias úteis, cabendo à contratada reapresentá-lo no prazo de até 3 dias úteis.

5.7. O plano deverá conter, ainda, a previsão de eventos que afetem outras atividades do Conselho ou que possam interagir com outros serviços e/ou dispositivos já em operação.

5.8. É parte integrante do plano a descrição contendo as principais funcionalidades dos itens contratados, também na forma sumária e o local de entrega; a documentação deverá ser aprovada pela equipe técnica do CFA;

5.9. Todos os serviços necessários à instalação e a configuração da solução proposta ficarão às custas da Contratada e deverão ser descritos no plano de execução, contendo a designação da quantidade necessária de técnicos especializados, fornecidos e mantidos pela Contratada, para a execução dos serviços;

5.10. Não será permitida a inclusão de funcionalidades, características de ambiente ou quaisquer outras que desvirtuem os requisitos da solução Contratada;

5.11. A instalação deverá ser efetuada de forma a não comprometer o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação no Conselho;

5.12. Havendo necessidade de interrupção de sistemas, recursos, equipamentos ou da rotina dos trabalhos de qualquer setor funcional em decorrência da instalação a ser efetuada, esta deverá ser devidamente planejada e necessariamente aprovada pela equipe técnica do CFA;

5.13. Para a execução dos serviços fica estabelecido o horário de funcionamento normal do CFA. Em caso de necessidade de interrupção de sistemas, recursos, equipamentos ou da rotina dos trabalhos, as atividades poderão ser planejadas e executadas fora do horário normal de expediente a critério da equipe técnica do CFA;

5.14. A Contratada devera elaborar Relatório Técnico analisando os resultados e entregá-lo a equipe técnica do CFA, para que ateste a conclusão da instalação e configuração;

5.15. Caberá ao CFA determinar o local onde os ativos serão instalados, assim como fornecer a estrutura elétrica e os racks 19" quando necessários, para acomodação e ligação dos equipamentos.

6. DO TREINAMENTO

6.1. A Contratada deverá ministrar treinamento relativo à instalação, gerenciamento, operacionalização, manuseio, configuração e utilização dos equipamentos fornecidos e seus componentes, visando garantir a transferência de conhecimento para até 5 (cinco) pessoas indicadas pelo Contratante;

6.2. O treinamento deverá possuir carga horária mínima adequada para abordar todo o conteúdo descrito no item anterior;

6.3. O treinamento deverá estar incluído no plano de execução proposto pela contratada, com a data de realização acordada com a contratante.

6.4. A Contratada deverá fornecer ambiente para realização do treinamento, com infraestrutura e material adequado para ministração. Poderão ser utilizados os equipamentos a serem fornecidos (se necessário);

6.5. O treinamento deverá ser credenciado e autorizado pelo fabricante da solução, devendo ser apresentado, em até 5 (cinco) dias úteis antes do início do treinamento, o conteúdo programático, a carga horária, nome e currículo do instrutor e o local de realização do treinamento;

6.6. Deverão ser utilizados material didático, um por participante e o instrutor deverá possuir experiência em treinamentos desta natureza e pleno conhecimento dos equipamentos. O material didático devera ser fornecidas também em mídia digital;

6.7. O treinamento deverá ser ministrado em Brasília-DF ou, no caso de ser ofertado em outra localidade, a Contratada deverá arcar com despesas de transporte, hospedagem e alimentação para os participantes indicados pelo CFA;

6.8. Deverá ser emitido certificado aos participantes do treinamento que cumprirem frequência mínima de 80%;

7. DA GARANTIA, SERVIÇO DE ASSISTÊNCIA TÉCNICA E OPERAÇÃO ASSISTIDA

7.1. O período de Garantia Técnica para todos os equipamentos, seus componentes (hardware e software) e serviços que compõem a solução, deverá ser de no mínimo 36 (trinta e seis) meses, contados a partir da data do recebimento definitivo;

7.2. **O valor referente a garantia, serviço de assistência técnica e operação assistida devem ser inclusos nos valores apresentados para solução;**

7.3. A Contratada deverá disponibilizar número telefônico e correio eletrônico para abertura de chamados de assistência técnica da garantia 24 x 7 x 365 (vinte e quatro horas por dia, sete dias por semana e trezentos e sessenta e cinco dias por ano);

7.4. A Contratada deverá também disponibilizar número telefônico e correio eletrônico para consultas técnicas do Contratante sobre as funcionalidades e a correta

utilização dos equipamentos e software, nos dias úteis (segunda-feira a sexta-feira), em horário comercial (08h às 18h);

7.5. Os custos telefônicos serão de responsabilidade da Contratada através de telefones tipo 0800 ou chamada a cobrar, caso não seja fornecido número local em Brasília-DF;

7.6. O atendimento de chamados de assistência técnica da garantia será do tipo "on site", mediante manutenção corretiva nas dependências do CFA no Distrito Federal, e deverá cobrir todo e qualquer defeito apresentado, incluindo o fornecimento e a substituição de peças e/ou componentes, ajustes, reparos e correções necessárias para recolocar os equipamentos e software em perfeito estado de funcionamento;

7.7. O atendimento de um chamado deverá ter início em até 2 (duas) horas corridas, contadas a partir do registro da solicitação. O prazo máximo para solução dos problemas reportados deverá ser de 24 (vinte e quatro) horas corridas, contadas a partir do registro da solicitação, excetuando-se no caso em que o problema constatado, acarretar indisponibilidade total nos acessos e serviços do CFA que dependam dos seus links de comunicação como acesso internet, email, publicações, sistemas web dentre outros, passando neste caso, o prazo máximo de solução para até 4 (quatro) horas;

7.8. Caso o problema não possa ser resolvido por meio de manutenção corretiva, componentes defeituosos deverão ser substituídos por outros com as mesmas funcionalidades dentro do prazo de 48 (quarenta e oito) horas corridas, contadas a partir do registro da solicitação;

7.9. O Contratante poderá efetuar um número ilimitado de chamados técnicos, durante o período da garantia, para correção de problemas relativos ao uso e aplicações dos equipamentos, software e suas funcionalidades;

7.10. Antes do fechamento de cada chamado a Contratada deverá consultar o CFA quanto à efetiva solução do problema em questão. Qualquer chamado fechado, sem anuência do CFA ou sem que o problema tenha sido resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas;

7.11. A Contratada manterá cadastro das pessoas indicadas pelo CFA que poderão efetuar abertura e autorizar o fechamento de chamados;

7.12. Ao término de atendimentos relacionados à assistência técnica da garantia, a Contratada deverá apresentar Relatório de Atendimento contendo data e hora da abertura do chamado, data e hora do início e do término do atendimento, identificação do defeito, nome do técnico responsável pela execução da garantia, providências adotadas e outras informações pertinentes. O Relatório deverá ser assinado por técnico do CFA;

7.13. A Contratada deverá substituir, em até 24 (vinte e quatro) horas, o equipamento/componente já instalado por um novo, sem ônus para o CFA, quando comprovados defeitos de fabricação, do próprio ou de seus componentes, que comprometa o seu desempenho, nas seguintes hipóteses: caso ocorram 4 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias; caso a soma dos tempos de paralisação do equipamento/componente ultrapasse 40 (quarenta) horas, dentro de qualquer intervalo de 30 (trinta) dias;

7.14. Respostas a consultas técnicas deverão ser respondidas em até 2 dias úteis contados a partir do dia de registro da solicitação;

7.15. O CFA reserva-se o direito de realizar a conexão ou instalação dos equipamentos em produtos de hardware de outros fornecedores ou fabricantes, sem que isto possa ser usado como pretexto pela Contratada para se desobrigar da garantia de funcionamento prevista nesta Especificação Técnica;

7.16. O atendimento deve ser efetuado em língua portuguesa;

7.17. A assistência técnica prestada tem validade de 36 (trinta e seis) meses e está inclusa no valor do equipamento adquirido;

7.18. O Fabricante deverá fornecer *drivers* e *firmware*, incluindo atualizações de versões e pequenas atualizações de release e reparos de defeitos (*bug fixing patches*) por 36 (trinta e seis) meses;

7.19. Entende-se por garantia a continuidade do funcionamento da solução sendo adquirido por 36 (trinta e seis) meses.

7.20. Além dos casos já citados, também são casos em que a garantia se aplica para substituição de equipamentos:

7.20.1. Falha de hardware e software que interrompa o funcionamento da ferramenta ou serviços providos ou utilizados pelo Conselho, por mais de 72 (setenta e duas) horas consecutivas;

7.20.2. Inoperância da ferramenta, por tempo superior a 72 (setenta e duas) horas corridas, em 2 (duas) ocasiões separadas por, no máximo, um período de 60 (sessenta) dias

corridos;

7.20.3. Funcionamento irregular, qualquer um que esteja em desacordo com o especificado pelo fabricante, em 2 (duas) ocasiões separadas por ate 60 (sessenta) dias corridos.

Operação Assistida

Por Operação Assistida entende-se, o conjunto de ações e atividades que permitam a habilitação, implementação/aplicação, manutenção e colocar em produção quaisquer funcionalidades da solução exigidas nas especificações técnicas deste Termo.

Através da Operação Assistida, também é possível promover a transferência de conhecimento e experiência necessária para a operação da solução (equipamentos, sistemas ou plataformas de serviços).

Durante as ações de Operação Assistida, a Contratada deverá prover um corpo técnico formado por um ou mais especialistas, que serão designados para atuação local no ambiente do Conselho, de modo a executar ações diretas de implementação de funcionalidades e/ou fornecimento de suporte na realização de testes, análises, medidas e ajustes, assegurando que a Solução contratada, opere em conformidade com os padrões pré-estabelecidos e demandados pela equipe técnica do CFA.

7.21. A Operação Assistida deverá estar disponível durante todo o período de garantia para todos os equipamentos, seus componentes e serviços que compõem a solução;

7.22. A Contratada deverá disponibilizar número telefônico e correio eletrônico para abertura de chamados de Operação Assistida, nos dias úteis (segunda feira a sexta-feira), em horário comercial (08h às 18h);

7.23. Os custos telefônicos serão de responsabilidade da Contratada através de telefones tipo 0800 ou chamada a cobrar, caso não seja fornecido número local em Brasília-DF;

7.24. O atendimento de um chamado deverá ter início em até 48 (quarenta e oito) horas corridas, contadas a partir do registro da solicitação;

7.25. A Contratada manterá cadastro das pessoas indicadas pelo CFA que poderão efetuar abertura e autorizar o fechamento de chamados;

7.26. O Contratante poderá efetuar, a seu critério, a abertura de até 30 chamados, a título de operação assistida, durante a vigência da garantia;

7.26.1. Cada chamado deverá conter um descritivo detalhado sobre a demanda a ser atendida e/ou funcionalidade a ser implementada;

7.26.2. O atendimento aos chamados de Operação Assistida deverá ser feito após planejamento acordado e aprovado pela equipe técnica do CFA;

7.26.3. A critério do Conselho, o atendimento a esta modalidade de chamado poderá ser realizada fora do horário de expediente normal do CFA em função dos impactos aos demais serviços em produção;

7.26.4. O atendimento deverá ser preferencialmente “on-site”, nas dependências do CFA, ficando facultado ao Contratante o fornecimento ou não, de acesso remoto a Contratada para realização das atividades;

7.26.5. A Contratada não poderá caracterizar como Operação Assistida quaisquer atividades/ações ou chamados cobertos pela Garantia e/ou Assistência Técnica;

7.26.6. Ao final de cada atendimento, deverá ser fornecido pela Contratada, relatório técnico detalhado e explicativo das atividades realizadas, a fim de promover a transferência de conhecimento à equipe técnica do Conselho;

7.26.7. Antes do fechamento de cada chamado, a Contratada deverá consultar o CFA quanto ao efetivo atendimento da demanda relacionada a ele. Qualquer chamado fechado, sem anuência do CFA ou sem que a demanda tenha sido atendida, será reaberto e aplicadas das sanções previstas como descumprimento contratual;

7.26.8. A contratante se reserva o direito de efetuar a avaliação do processo de atendimento do Serviço de Operação Assistida e caso o repasse de informações não tenha sido realizado de forma satisfatória, a contratada deverá repassar os processos necessários até o total esclarecimento de eventuais dúvidas apresentadas quanto às atividades realizadas;

7.26.9. Cada chamado de Operação Assistida, corresponderá a 8 horas ou um dia útil de atendimento, ficando a critério da Contratada a alocação do quantitativo de técnicos e equipe suficiente para sua execução completa da atividade demandada.Será utilizado como critério de validação do atendimento, a entrega do relatório final de execução, repasse de conhecimento e ateste da equipe técnica do CFA quanto a conformidade da implementação com a demanda estabelecida.

8. DOS PRAZOS E CONDIÇÕES PARA ENTREGA DO OBJETO

8.1. O prazo máximo de entrega da solução é de até 45 (quarenta e cinco) dias corridos, contados a partir da data de assinatura do contrato.

8.2. O prazo máximo para instalação, configuração e customização da solução é de até 60 (sessenta) dias corridos contados a partir da data de assinatura do contrato.

8.3. A Contratada deverá apresentar os produtos acondicionados conforme padrão do fabricante devendo garantir a proteção durante o transporte e estocagem, bem como deve constar nas caixas a identificação dos produtos e demais informações exigidas na legislação em vigor.

8.4. A entrega dos equipamentos deverá ser feita na coordenadoria de informática do CFA.

9. DA CAPACIDADE TÉCNICA

9.1. Pelo menos um atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado e apresentado em papel timbrado do emitente, contendo o nome da empresa, a identificação dos signatários, endereço completo, telefone, e se for o caso, correio eletrônico, para contato, que comprovem aptidão para desempenho de atividade pertinente e compatível com o objeto deste Termo de Referência. Cada atestado entregue deverá estar acompanhado de cópia autenticada do respectivo contrato;

10. DAS OBRIGAÇÕES DAS PARTES

10.1. A **CONTRATANTE** obriga-se a:

10.1.1. Acompanhar e fiscalizar a execução do contrato, através de servidor designado para este fim, nos termos do art. 67 da Lei nº 8.666/93.

10.1.2. Atentar para que durante a vigência do presente contrato seja mantida a situação de regularidade relativa à seguridade social (INSS), ao Fundo de Garantia por Tempo de Serviço (FGTS) e a Fazenda Federal da CONTRATADA, bem assim a sua compatibilidade com as obrigações assumidas pela CONTRATADA.

10.1.3. Efetuar o pagamento nas condições e preços ajustados, após o devido atesto da nota fiscal/fatura.

10.1.4. Transmitir ao preposto da Contratada toda e qualquer demanda.

10.1.5. Aplicar à Contratada as penalidades regulamentares e contratuais.

10.1.6. Designar responsável para o acompanhamento e fiscalização da execução do objeto deste Termo de Referência.

10.1.7. Prestar as informações e esclarecimentos necessários à CONTRATADA.

10.1.8. Responder pelas consequências de suas ações ou omissões.

10.1.9. Comunicar à Contratada quaisquer ocorrências relacionadas com a execução do(s) serviço(s).

10.2. a **CONTRATADA** obriga-se a:

10.2.1. Nomear preposto para acompanhamento da prestação dos serviços, que deverá seguir as orientações demandadas pelo CFA.

10.2.2. Assumir todos e quaisquer ônus, referente a salário, horas extras, adicionais e demais encargos sociais relativamente aos seus empregados; assumir a responsabilidade pelos encargos fiscais e comerciais resultante da adjudicação desta Licitação.

10.2.3. Manter, durante toda a execução do serviço, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

10.2.4. Zelar pela perfeita execução dos serviços.

10.2.5. Prover, realizar, manter e priorizar todas as ações necessárias ao fiel cumprimento das cláusulas contidas neste Termo de Referência.

10.2.6. Prestar os serviços de forma meticulosa e constante, mantendo-os sempre em perfeita ordem.

10.2.7. Arcar com eventuais prejuízos causados ao CFA ou a terceiros, provocados por negligência ou irregularidade cometida por seus empregados ou prepostos envolvidos na execução do objeto.

10.2.8. Responsabilizar-se por todas as despesas diretas ou indiretas, tais como: salários, transportes, encargos sociais, fiscais, trabalhistas, previdenciários e de ordem de classe, indenizações e quaisquer outras que forem devidas aos seus empregados no desempenho dos serviços objeto do contrato, ficando a CONTRATANTE isenta de qualquer vínculo empregatício com os mesmos.

10.2.9. Entregar os serviços nos prazos e condições especificados.

10.2.10. Manter seus empregados e/ou prepostos, quando em serviço, devidamente identificados, mediante o uso permanente de crachás.

10.2.11. Providenciar a imediata correção das deficiências, falhas ou irregularidades apontadas pela CONTRATANTE.

11. DA FISCALIZAÇÃO E CONTROLE

11.1. Não obstante a EMPRESA VENCEDORA DA LICITAÇÃO seja a única e exclusiva responsável pela execução de todos os serviços, o CONSELHO FEDERAL DE ADMINISTRAÇÃO reserva-se o direito de, sem que de qualquer forma restrinja a plenitude desta responsabilidade, exercer a mais ampla e completa fiscalização sobre os serviços, por colaborador a ser designado por portaria.

12. DAS SANÇÕES E PENALIDADES

12.1. O licitante vencedor que descumprir quaisquer das cláusulas ou condições do presente edital ficará sujeito às penalidades previstas nas Leis nº 10.520/2002 e 8.666/93.

12.2. Conforme o disposto no art. 28 do Decreto nº 5.450, de 31/05/2005, o licitante vencedor que, dentro do prazo de validade de sua proposta, negar-se a retirar a nota de empenho, deixar de assinar o termo de contrato quando exigido, deixar de entregar a documentação exigida para o certame ou apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedido de licitar e contratar com a União, e, se for o caso, será descredenciado no SICAF, pelo prazo de até 5 anos, sem prejuízo das multas previstas neste edital e das demais cominações legais.

12.3. Além do previsto no subitem anterior, pelo descumprimento total ou parcial das obrigações assumidas e pela verificação de quaisquer das situações previstas no art. 78, incisos I a XI da Lei 8.666/93, a Administração poderá, resguardados os procedimentos legais pertinentes, aplicar as seguintes sanções, conforme art. 87 da Lei 8.666/93, sem prejuízo de outras:

12.3.1. advertência;

12.3.2. multa, a ser recolhida no prazo máximo de 5 (cinco) dias úteis, a contar da comunicação oficial, nas seguintes hipóteses:

12.3.2.1. 0,3% (três décimos por cento) sobre o valor total da contratação, caso a CONTRATADA não forneça os produtos e demais condições avençadas no prazo, por dia de atraso injustificado, limitada sua aplicação até o máximo de 30 (trinta) dias. Após o 30º dia de atraso, os serviços poderão, a critério da Administração, não mais ser aceitos, configurando-se a inexecução do contrato.

12.3.2.2. Em caso de atraso na entrega da solução, será cobrada multa no valor de 0,3% por dia de atraso, calculada sobre o valor total dos produtos em mora, limitada a 30 (trinta) dias. A mesma multa será aplicada para o caso de atraso na prestação dos serviços de instalação, configuração e customização.

12.3.2.3. Em caso de atraso no atendimento de chamados de assistência técnica, será cobrada multa no valor de valor de 0,5% por hora de atraso para cada chamado não solucionado, calculada sobre o valor da solução, limitada a 24 (vinte e quatro) horas. Poderá haver mais de um chamado aberto simultaneamente, razão pela qual poderá haver a cobrança cumulativa de multas sobre o atraso no atendimento.

12.3.2.4. Em caso de atraso na resposta a consultas técnicas e chamados de Operação Assistida, será cobrada multa no valor de valor de 0,05% por dia de atraso para cada consulta não respondida, calculada sobre o valor total do contrato, limitada a 20 (vinte) dias. Poderá haver mais de uma consulta aberta simultaneamente, razão pela qual poderá haver a cobrança cumulativa de multas sobre o atraso na resposta.

12.3.2.5. Caso sejam excedidos os prazos limites estipulados nos itens anteriores, será considerado descumprimento parcial do contrato, sendo aplicadas as penalidades previstas para tal ocorrência, além da multa estipulada no item originalmente descumprido.

12.3.2.6. Em caso de atraso na resposta a consultas técnicas e chamados de Operação Assistida, será cobrada multa no valor de 0,05% (cinco centésimos por cento) por dias de atraso para cada consulta não respondida, calculada sobre o valor total do contrato, limitada a 20 (vinte) dias. Poderá haver mais de uma consulta aberta simultaneamente, razão pela qual poderá haver a cobrança cumulativa de multas sobre o atraso na resposta.

12.3.2.7. Em caso de atraso no atendimento de chamados de assistência técnica, será cobrada multa no valor de 0,5% (cinco décimos por cento) por hora de atraso para cada chamado não solucionado, calculada sobre o valor da solução, limitada a 20 (vinte) dias. Poderá haver mais de um chamado aberto simultaneamente, razão pela qual poderá haver a cobrança cumulativa de multa sobre o atraso no atendimento.

12.3.2.8. 10% (dez por cento) sobre o valor deste CONTRATO, em caso de rescisão

causada por ação ou omissão injustificada da CONTRATADA.

12.3.2.9. 10% (dez por cento) sobre o valor total do Contrato, no caso de inexecução total do contrato.

12.3.3. suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por até 2 (dois) anos;

12.3.4. declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a licitante vencedora ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

12.4. As penalidades previstas neste Edital são independentes entre si, podendo ser aplicadas isoladas ou, no caso de multa, cumulativamente, sem prejuízo de outras medidas cabíveis, garantida prévia defesa (art. 87, § 2º, da Lei nº 8.666/93).

12.5. No caso de não-recolhimento do valor da multa, dentro de 5 (cinco) dias úteis a contar da data da intimação para o pagamento, a importância será descontada da garantia prestada ou dos pagamentos a que fizer jus a CONTRATADA ou ajuizada a dívida, consoante o § 3º do art. 86 e § 1º do art. 87 da Lei n.º 8.666/93, acrescida de juros moratórios de 1,0% (um por cento) ao mês.

12.6. A aplicação das sanções previstas neste CONTRATO não exclui a possibilidade da responsabilidade civil da CONTRATADA por eventuais perdas e danos causados à Administração Pública.

12.7. Os atos administrativos de aplicação das sanções previstas nos incisos III e IV, do art. 87, da Lei n.º 8.666/93 e a constantes do art. 7º da Lei nº 10.520/02, bem como a rescisão contratual, serão publicados resumidamente no Diário Oficial da União.

12.8. De acordo com o artigo 88, da Lei nº 8.666/93, serão aplicadas as sanções previstas nos incisos III e IV do artigo 87 da referida lei, à CONTRATADA ou aos profissionais que, em razão dos contratos regidos pela citada lei:

12.9. tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraudes fiscais no recolhimento de quaisquer tributos;

12.10. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

12.11. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

12.12. Da aplicação das penas definidas no § 1º e no art. 87, da Lei n.º 8.666/93, exceto para aquela definida no inciso IV, caberá recurso no prazo de 05(cinco) dias úteis da data de intimação do ato.

12.13. No caso de declaração de inidoneidade, prevista no inciso IV, do art. 87, da Lei n.º 8.666/93, caberá pedido de reconsideração ao Exmo. Sr. Presidente do Conselho Federal de Administração, no prazo de 10 (dez) dias úteis a contar da data de intimação do ato, podendo a reabilitação ser requerida após 2 (dois) anos de sua aplicação.

12.14. Na comunicação da aplicação da penalidade de que trata o item anterior, serão informados o nome e a lotação da autoridade que aplicou a sanção, bem como daquela competente para decidir sobre o recurso.

12.15. O recurso e o pedido de reconsideração deverão ser entregues, mediante recibo, no setor de protocolo do CONTRATANTE, localizado no edifício CFA, situado no Setor de Autarquias Sul, Quadra 01 Bloco L, Brasília/DF, nos dias úteis, das 14h às 17h.

13. DA DOTAÇÃO ORÇAMENTÁRIA

13.1. Os recursos para custeio das despesas decorrentes da contratação que se seguir à licitação de que trata este Termo de Referência, correrão à conta das seguintes Dotações Orçamentárias nºs 6.2.2.1.1.02.02.03.003/6.2.2.1.1.02.02.03.005

14. DOS CUSTOS ESTIMADOS

14.1. O valor global estimado para gastos será de R$ 161.426,00 (cento e sessenta e um mil quatrocentos e vinte seis reais).

15. DO PAGAMENTO E PRAZO DE VIGÊNCIA DO CONTRATO

15.1. Os pagamentos à adjudicatária que vier a ser contratada para a execução do objeto desta licitação serão feitos nos termos abaixo, consoantes os percentuais estabelecidos na Proposta final.

15.2. Os valores dos fornecimentos sujeitam-se às seguintes regras:

15.3. Os valores dos de que trata o objeto deste termo, compreenderão o valor dos serviços contratados pela licitante vencedora, acrescido da taxa de administração, quando

for o caso.

15.4. O pagamento fica condicionado à prévia certificação quanto à execução a contento dos serviços e entrega de produtos

15.5. Não serão efetuados quaisquer pagamentos enquanto perdurar pendência de liquidação de obrigações, em virtude de penalidades impostas à CONTRATADA, ou inadimplência contratual.

15.6. A liberação do pagamento ficará condicionada à comprovação da regularidade fiscal da CONTRATADA, além da regularidade junto ao INSS e ao FGTS, mediante consulta efetuada por meio eletrônico ou por meio da apresentação de documentos hábeis.

15.7. Encontrando-se a empresa contratada inadimplente na data da consulta, poderá ser concedido, a critério do CFA, prazo de até 15 (quinze) dias para que a empresa regularize a sua situação, sob pena de, não o fazendo, ter o contrato rescindido com aplicação das sanções cabíveis.

15.8. A CONTRATADA deverá apresentar em sua Nota Fiscal/Fatura exclusivamente o faturamento detalhado correspondente ao objeto autorizado, mediante contrato especifico. Havendo erro ou circunstância que impeça a liquidação da despesa, aquela será devolvida à CONTRATADA e o pagamento ficará pendente até que seja sanado o problema. Nesta hipótese, o prazo para pagamento será reiniciado após a regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para o CFA.

15.9. O CFA reserva-se o direito de não efetuar o pagamento se, no ato da atestação, a prestação dos serviços ou entrega de produtos não estiver de acordo com a especificação exigida.

16. DO CRONOGRAMA DE EXECUÇÃO FÍSICO E FINANCEIRO

Do Local e do Prazo de Entrega

16.1. O objeto deverá ser entregue na sede do CFA, localizado no Setor de Autarquias Sul - SAUS, Quadra 1, Bloco L, CEP 70070-932, em dias úteis, de 09h00 às 17h00;

16.2. Os equipamentos que compõem a solução, deverão ser novos, entregues em perfeito estado de funcionamento, sem marcas, sem arranhões ou amassados.

Do Recebimento

16.3. O recebimento do objeto se dará, provisoriamente, no ato da entrega na coordenadoria de informática do CFA para posterior verificação da conformidade com as especificações contidas neste termo de referência.

16.4. O recebimento definitivo se dará em até 30 (trinta) dias após verificação de que a solução foi entregue de acordo com as condições e as especificações deste Termo de Referência, além de configurada e customizada, de acordo com o plano de execução entregue pela contratada e atestado pela equipe técnica do CFA.

Entregáveis

Item	Data	Pagamento	Responsável
Assinatura do Contrato	D	Não aplicável	Contratante/Contratada
Plano de Execução	Até D+10	Não aplicável	Contratada
Termo de Recebimento Provisório	Até D+45	Não aplicável	Contratante
Instalação, Configuração e Customização	Até D+60	Não aplicável	Contratada
Treinamento	Até D+60	Não aplicável	Contratada
Termo de Recebimento Definitivo	Até D+90	Aplicável em até 30 dias após emissão da fatura	Contratante

Documento assinado eletronicamente por **Marcos Antonio Susin**, **Analista de Banco de Dados**, em 11/06/2019, às 10:29, conforme horário oficial de Brasília.

A autenticidade deste documento pode ser conferida no site sei.cfa.org.br/conferir, informando o código verificador **0287626** e o código CRC **DA26E625**.

1.