**SERVIÇO PÚBLICO FEDERAL**
CONSELHO FEDERAL DE QUÍMICA
**SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE**
**70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br**

**ANEXO I**

**TERMO DE REFERÊNCIA**

PROCESSO ADMINISTRATIVO N° 22/2020

1.1. Contratação de empresa especializada para o fornecimento de solução de Firewall, incluindo instalação, suporte técnico, repasse de conhecimento, garantia, conforme condições, quantidades e exigências estabelecidas neste instrumento:

| ITEM | DESCRIÇÃO/ ESPECIFICAÇÃO | CATMAT | Unidade de Medida | Quantidade | Valor Máximo Aceitável |
|---|---|---|---|---|---|
| 1 | Contratação de empresa especializada para o fornecimento de solução de Firewall, Implantação e Configuração, repasse de conhecimento, garantia e Suporte Técnico de 36 meses | 150100 | Unidade | 1 | R$ 79.466,21 (setenta e nove mil, quatrocentos e sessenta e seis reais e vinte e um centavos) |

1.2. O objeto da licitação enquadra-se na categoria de bens comuns, por possuir padrões de desempenho e características gerais e especificas, que podem ser definidas de forma objetiva nas especificações técnicas, que são usualmente encontradas no mercado, podendo, portanto, ser licitado por meio da modalidade Pregão.
1.3. Os quantitativos e respectivos códigos dos itens são os discriminados na tabela acima.
1.4. A presente contratação adotará como regime de execução a Empreitada por Preço Global.
1.5. O contrato terá vigência pelo período de 105 (cento e cinco dias).

**JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO**

1.6. A Justificativa e o objetivo da contratação encontram-se pormenorizados em Tópico específico dos Estudos Preliminares, apêndice desse Termo de Referência.
1.7. O firewall é um sistema, configurado pelos administradores, que permite liberar ou bloquear o tráfego passante entre redes. As regras de liberação e bloqueio são necessárias para se bloquear acessos indevidos a sistemas e redes e, devem sempre seguir o princípio do privilégio mínimo.
1.8. O firewall representa um quesito de segurança fundamental, uma vez que regula o tráfego de dados entre redes distintas e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede.

**DESCRIÇÃO DA SOLUÇÃO:**

1.9. A descrição da solução como um todo, conforme minudenciado nos Estudos Preliminares e abrange:
aquisição de solução de segurança da Informação (Firewall), para proteção rede de dados nos termos do item deste documento.
1.9.1. A implantação proporcionará agilidade ao processo de implantação deste equipamento no Conselho Federal de Química, aumentando a confiabilidade do controle, facilitando a junção das informações através de painel único que centraliza as informações de segurança no CFQ. Por tratar-se de uma ferramenta institucional, deverá ser garantida a continuidade do suporte técnico e a atualização das suas funcionalidades de modo que seja possível lidar com o surgimento de novas exigências. O sistema deverá proporcionar consciência situacional sobre as vulnerabilidades e malwares que afetam a segurança da informação no Conselho Federal de Química.
1.9.2. Com relação ao treinamento padronizado, este propiciará a disseminação única das informações de segurança, a forma de trabalho padronizada, a forma de intercâmbio e da divulgação das vulnerabilidades.
1.9.3. Por fim, a garantia única para toda a solução de segurança da informação (firewall) permitirá a correção padronizada e única de possível incorreções na solução, aplicada de forma centralizada, permitindo uma coordenação direta com a empresa responsável.
1.9.4. A entrega e instalação do equipamento deverá ocorrer no seguinte endereço: Setor Comercial Sul, Quadra 9, bloco A, Torre B, 9° andar - Edifício Parque Cidade Corporate, Asa Sul, Brasília/DF – CEP: 70.308-200. A Contratada deverá agendar previamente sua realização junto a Gerência de Tecnologia da Informação (61) 2099-3366 e 3360, Email: euripedes.rocha@cfq.org.br ou cristiano.ferreira@cfq.org.br.

**DA CLASSIFICAÇÃO DOS SERVIÇOS E FORMA DE SELEÇÃO DO FORNECEDOR**

1.10. Trata-se de serviço comum de caráter continuado sem fornecimento de mão de obra em regime de dedicação exclusiva, a ser contratado mediante licitação, na modalidade pregão, em sua forma eletrônica.

1.11. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto n° 9.507, de 21 de setembro de 2018, não se constituindo em quaisquer das atividades, previstas no art. 3º do aludido decreto, cuja execução indireta é vedada.

1.12. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

**REQUISITOS DA CONTRATAÇÃO**

1.13 Conforme Estudos Preliminares, os requisitos da contratação abrangem o seguinte:

1.13.1 Gerenciamento centralizado, visando manter o controle das funcionalidades e regras em uma plataforma única, podendo ser acessado remotamente;

1.13.2 Atendimento para qualquer incidente no ambiente de segurança da informação, trazendo autonomia para a equipe de TI (Tecnologia da Informação) desenvolver novos projetos de segurança e manter a produção do firewall adquirido;

1.13.3 Diminuição do risco operacional da Infraestrutura de TI visando o aumento da eficiência de monitoração de eventos cibernéticos e o atingimento dos índices de eficiência e segurança previstos;

1.13.4 Monitoramento do ambiente e colaboração interna, com aplicações de ações preventivas e corretivas, sanando eventuais irregularidades, incluindo avaliação frequente de capacidade dos equipamentos;

1.13.5 Melhoria da integração entre as áreas e por consequência diminuição dos custos com a Gestão da Segurança da Informação;

1.13.6 Melhoria da sensibilidade da organização a respeito de tomadas de decisões frente às incertezas e qualquer tipo de indício de oportunidade ou ameaça a ser tratada;

1.13.7 A licitante deverá declarar que tem pleno conhecimento das condições necessárias para a prestação do serviço sendo os custos com hospedagem e deslocamento da contratada serão por conta própria da contratada;

1.13.8 As empresas licitantes deverão declarar formalmente que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto na Lei n nº 8.666/93.

1.13.9 As obrigações da Contratada e Contratante estão previstas neste TR;

1.13.10 Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 09:00 horas às 17:00 horas.

1.13.11 O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.

1.13.12 Para a vistoria o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

## 2. MODELO DE EXECUÇÃO DO OBJETO

2.1. A execução do objeto seguirá a seguinte dinâmica:

2.2. **Aquisição de Solução de Segurança de Informação, Firewall**

2.2.1. A aquisição de solução de segurança da Informação (Firewall), para proteção rede de dados considerar os seguintes fatores:

a) Manter segurança da informação entre todos dispositivos conectados entra a rede LAN e WAN dentro das instalações do conselho Federal de Química
b) Possibilidade Conectividade, mobilidade e estabilidade;
c) Manutenção e suporte técnico facilitado;
d) Vantajosidade para o CFQ, quanto ao custo;
e) Facilidade no escalonamento da solução;
f) Aplicabilidade das políticas de segurança da Informação do CFQ.

2.3. **Descrição da Solução - Firewall**

2.3.1. Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para 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, malwares, Filtro de URL, criptografia de email, inspeção de tráfego criptografado e proteção de firewall de aplicação Web.

2.3.2. Console de gerenciamento dos equipamentos e centralização de logs em hardware específico ou virtualizado.

2.3.3. Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus / malwares, endpoints, softwares de criptografia de armazenamento em nuvem e assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, pelo período mínimo de 36 (trinta e seis) meses.

2.3.4. Para os itens que representem bens materiais, a CONTRATADA deverá fornecer produtos novos, sem uso anterior.

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

2.3.6. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

2.3.7. A solução deverá contemplar a totalidade das capacidades exigidas, sendo permitido o uso de um equipamento para a solução.

2.3.8. Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.

2.3.9. O hardware e o software fornecidos não podem 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.

2.4. **Características Específicas De Hardware considerando as funcionalidades de Next Generation**

2.4.1. Performance mínima de 1.5 Gbps de throughput para firewall.

2.4.2. Performance mínima de 4 Gbps de throughput de IPS.

2.4.3. Performance mínima de 2Gbps de throughput para controle de AV/proxy.

2.4.4. Performance mínima de 1.5 Gbps de throughput de VPN.

2.4.5. Suporte a, no mínimo, 300.000 de conexões simultâneas.

2.4.6. Suporte a, no mínimo, 300.000 novas conexões por segundo.

2.4.7. Possuir o número irrestrito quanto ao máximo de usuários licenciados.

2.4.8. Possuir armazenamento interno de no mínimo 480 GB SSD (RAID-1) hot-swap para sistema operacional, quarentena local, logs e relatórios.

2.4.9. Possuir no mínimo 64GB de memória RAM.

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

2.4.11. Possuir no mínimo 8 (oito) módulo de expansão de interfaces com até 64 (sessenta e quatro) interfaces de rede 1000Base-TX instaladas.

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

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

2.5. **Características Gerais Para Firewalls De Próxima Geração**

2.5.1. Solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência, monitoração e logs.

2.5.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

2.5.3. 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.

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

2.5.5. O software deverá ser fornecido em sua versão mais atualizada.

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

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

2.5.8. O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.

2.5.9. O backup e o reestabelecimento de configuração deverão ser feitos localmente, via FTP ou e-mail com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

2.5.10. As notificações deverão ser realizadas via e-mail e SNMP.

2.5.11. Suportar SNMP e Netflow.

2.5.12. O firewall deverá ser stateful, com inspeção profunda de pacotes (deep packet inspection).

2.5.13. As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.

2.5.14. As políticas de NAT deverão ser customizáveis para cada regra.

2.5.15. A proteção contra flood deverá ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS) e bloqueio de portscan.

2.5.16. Proteção contra anti-spoofing.
2.5.17. Suportar IPv4 e IPv6.
2.5.18. IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.
2.5.19. Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP).
2.5.20. Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.
2.5.21. O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso.
2.5.22. A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;
2.5.23. A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP;
2.5.24. O traffic shapping (QoS) deverá ser baseado em rede ou usuário.
2.5.25. A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.
2.5.26. Deve possuir otimização em tempo real de voz sobre IP.
2.5.27. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

2.6. **CONTROLE POR POLÍTICAS DE FIREWALL**

2.6.1. Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.
2.6.2. O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.
2.6.3. As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.
2.6.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
2.6.5. Controle de políticas por países via localização por IP.
2.6.6. Suporte a objetos e regras IPV6.
2.6.7. Suporte a objetos e regras multicast.

2.7. **PREVENÇÃO DE AMEAÇAS**

2.7.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, Anti-Malware e Firewall de Proteção Web (WAF) integrados no próprio appliance de Firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.
2.7.2. Deve realizar a inspeção profunda de pacotes (DPI deep packet inspection) para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).
2.7.3. As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.
2.7.4. Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;
2.7.5. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Malware, possibilitando a criação de diferentes politicas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;
2.7.6. A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-emails.
2.7.7. A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript.
2.7.8. Deve ter proteção em tempo real contra novas ameaças criadas.
2.7.9. Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente.
2.7.10. Deve permitir o bloqueio de vulnerabilidades.
2.7.11. Deve permitir o bloqueio de exploits conhecidos.
2.7.12. Deve detectar e bloquear o tráfego de rede que busque acesso a contact command e servidores de controle utilizando múltiplas camadas de DNS, AFC e firewall.
2.7.13. Deve incluir proteção contra ataques de negação de serviços.
2.7.14. Ser imune e capaz de impedir ataques básicos como: SYN flood, ICMP flood, UDP Flood, etc.
2.7.15. Suportar bloqueio de arquivos por tipo.
2.7.16. 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.
2.7.17. Os eventos devem identificar o país de onde partiu a ameaça.
2.7.18. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em 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, zonas de segurança.

2.7.19. 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.
2.7.20. 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.
2.7.21. O firewall de aplicação Web (WAF) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de performance do WAF e permissão e bloqueio de ranges de IP
2.7.22. Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a proteção da aplicação Web, podendo ser configuradas isoladamente ou simultaneamente.
2.7.23. Proteção pelo menos contra os seguintes ataques, mas não limitado a: SQL injection e Cross-site scripting.

2.8. **CONTROLE E PROTEÇÃO DE APLICAÇÕES**

2.8.1. Os dispositivos de proteção de rede deverão possuir a 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.
2.8.2. Reconhecer pelo menos 2.300 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 softwares.
2.8.3. Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.
2.8.4. Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Vídeo Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website)
2.8.5. O escaneamento de micro app deverá ser habilitado via console gráfica (GUI) e via comando de linha (CLI).
2.8.6. 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.
2.8.7. Atualizar a base de assinaturas de aplicações automaticamente.
2.8.8. Reconhecer aplicações em IPv6.
2.8.9. Limitar a banda usada por aplicações (traffic shaping).
2.8.10. 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.
2.8.11. 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.
2.8.12. Deve permitir o 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.

2.9. **CONTROLE E PROTEÇÃO WEB**

2.9.1. Deve permitir especificar 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 em uma única vez.
2.9.2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;
2.9.3. Deve incluir a 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;
2.9.4. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

2.9.5. Possuir pelo menos 90 categorias de URLs;
2.9.6. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
2.9.7. Deve ser capaz de forçar o uso da opção Safe Search em sites de busca;
2.9.8. Deve ser capaz 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 visível ao usuário;
2.9.9. Suportar a criação categorias de URLs customizadas;
2.9.10. Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.
2.9.11. Permitir a customização de página de bloqueio;
2.9.12. Suportar a inclusão nos logs do produto de informações das atividades dos usuários;
2.9.13. Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.
2.9.14. Deve realizar caching do conteúdo web;
2.9.15. Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

## 2.10. IDENTIFICAÇÃO DE USUÁRIOS

2.10.1. 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, autenticando via LDAP, Active Directory, Radius, eDirectory, TACACS+ e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.
2.10.2. 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).
2.10.3. 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.
2.10.4. 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.
2.10.5. Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory e eDirectory.
2.10.6. Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

## 2.11. QUALIDADE DE SERVIÇO – QoS

2.11.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.
2.11.2. 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.
2.11.3. Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado.
2.11.4. Suportar priorização Real-Time de protocolos de voz (VoIP).

## 2.12. REDES VIRTUAIS PRIVADAS - VPN

2.12.1. Suportar VPN Site-to-Site e Cliente-to-Site.
2.12.2. Suportar IPsec VPN.
2.12.3. Suportar SSL VPN.
2.12.4. Suportar L2TP e PPTP.
2.12.5. Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.
2.12.6. Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL para estações Windows.
2.12.7. Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.
2.12.8. 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.

2.12.9. 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).
2.12.10. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Dell SonicWALL, Fortinet, Huawei, Aruba, Extreme, Intelbras, Juniper, Palo Alto Networks e Sophos.
2.12.11. 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;
2.12.12. Suportar autenticação via AD/LDAP, Token e base de usuários local;
2.12.13. Permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, Active Directory, Radius, eDirectory, TACACS+ e via base de dados local;

2.13. **GERÊNCIA ADMINISTRATIVA CENTRALIZADA**

2.13.1. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.
2.13.2. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.
2.13.3. Estar licenciada para gerenciar as soluções de firewall de próxima geração.
2.13.4. Devem ser fornecidas soluções virtuais ou via appliances desde que obedeçam a todos os requisitos desta especificação.
2.13.5. Deve ser centralizada a gerencia de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração, sem necessidade de acesso direto aos equipamentos.
2.13.6. Deve permitir a criação de Templates para configurações.
2.13.7. Deve possuir indicadores do estado de equipamentos e rede.
2.13.8. 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.
2.13.9. Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.
2.13.10. Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc);
2.13.11. 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;
2.13.12. Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.
2.13.13. Deve ter integração com a 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.

2.14. **GERÊNCIA DE LOGS E RELATÓRIOS CENTRALIZADOS**

2.14.1. Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.
2.14.2. Estar licenciada para gerenciar as soluções de firewall de próxima geração.
2.14.3. Devem ser fornecidas soluções virtuais ou via appliances desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 1TB de dados.
2.14.4. Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.
2.14.5. Deve possibilitar a 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.
2.14.6. Deve conter relatórios pré-configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN;
2.14.7. Deve fornecer relatórios históricos para análises de mudanças e comportamentos.
2.14.8. Deve conter customizações dos relatórios para inserção de logotipos próprios.
2.14.9. Deve fornecer relatórios de compliance SOX, HIPAA e PCI.
2.14.10. Deve permitir a exportação via PDF ou Excel.
2.14.11. Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.
2.14.12. Deve fornecer relatórios de tendências.
2.14.13. Deve fornecer logs em tempo real, de auditoria e arquivados.
2.14.14. Deve possuir mecanismo de procura de logs arquivados.
2.14.15. Deve ter acesso baseado em Web com controles administrativos distintos.

2.15. **SERVIÇO DE INSTALAÇÃO**

2.15.1. Será feita instalação de 1 (um) firewall na sede do CFQ (Data Center Sul) como Perímetro na topologia da rede deste Conselho.
2.15.2. Todo cabeamento estruturado e instalação elétrica estão disponíveis no CFQ para alimentação de energia e conexão Ethernet nos equipamentos que serão instalados.
2.15.3. A troca da solução anterior pela nova, bem como qualquer configuração que interfira no atendimento do CFQ será realizado obrigatoriamente aos sábados ou durante a semana após às 19h, sem custos extras para o CFQ.

2.16. **SUPORTE TÉCNICO E GARANTIA**
2.16.1. Serviço de suporte e garantia no prazo de 36 meses, a contar da instalação, configuração e ativação do equipamento.
2.16.2. Caso haja necessidade de interrupção das funcionalidades do equipamento em prazo superior ao estabelecido no IMR a contratada deverá disponibilizar imediatamente equipamento de capacidade igual ou superior para uso do CFQ, a fim de evitar interrupções e prejuízos e danos a segurança a rede de dados deste Conselho.

2.17. **TREINAMENTO**
2.17.1 Repasse de conhecimento de todo gerenciamento da solução, incluindo relatórios, para 2 servidores do CFQ.
2.17.2 Modalidade Presencial Igual ou superior a 12 horas
2.17.3 Treinamento será agendado posteriormente a instalação da solução

| ITEM | DESCRIÇÃO | UNIDADE | QUANTIDADE |
|---|---|---|---|
| 1 | Equipamento – Firewall | Solução | 01 |
| 2 | Implantação e configuração | Serviço | 01 |
| 3 | Repasse de conhecimento | Serviço | 01 |
| 4 | Licença e suporte no período de 36 meses | Serviço | 01 |

2.17.4 A execução dos serviços contratados pressupõe a existência dos seguintes papeis e responsabilidades:
2.17.4.1 Gestor do Contrato: servidor designado pelo CONTRATANTE para coordenar e comandar o processo de gestão e fiscalização da execução contratual;
2.17.4.2 Fiscal Técnico do Contrato: servidor da área de Tecnologia da Informação designado pelo CONTRATANTE para a fiscalização técnica da execução contratual e pela verificação dos resultados pretendidos;
2.17.4.3 Fiscal Administrativo do Contrato: servidor da área Administrativa designado pelo CONTRATANTE para fiscalizar o Contrato quanto aos aspectos administrativos.
2.17.4.4 Preposto: funcionário representante da CONTRATADA, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal com o CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;
2.17.5 A execução do objeto obedecerá às etapas descritas na Tabela abaixo, e em seus respectivos prazos:

| | **Ativos de rede (Equipamentos)** |
|---|---|
| Etapas | 1ª) Entrega do Equipamento – Firewall;<br><br>2ª) Fornecimento de serviço de instalação e configuração<br><br>3ª) Repasse de conhecimento da solução;<br><br>4ª) Prestação de serviço de Garantia e Suporte Técnico, durante 36 (trinta e seis) meses; |
| Prazo de entrega do equipamento ou material | Até 60 (sessenta) dias corridos, da data de assinatura da ordem de serviço |
| Prazo de Vigência do Contrato | 105 (cento e cinco) dias |
| Considerações Adicionais | 36 meses de suporte e garantia |

## 3 OBRIGAÇÕES DA CONTRATANTE

3.1 Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

3.2 Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

3.3 Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;

3.4 Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;

3.5 Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da contratada, no que couber, em conformidade com o item 6 do Anexo XI da IN SEGES/MP n. 5/2017.

3.6 Não praticar atos de ingerência na administração da Contratada, tais como:

3.7 exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação previr o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;

3.8 direcionar a contratação de pessoas para trabalhar nas empresas Contratadas;

3.9 considerar os trabalhadores da Contratada como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens.

3.10 Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;

3.11 Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

3.12 Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento das obrigações pela Contratada;

3.13 Arquivar, entre outros documentos, projetos, "as built", especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas;

3.14 Fiscalizar o cumprimento dos requisitos legais, quando a contratada houver se beneficiado da preferência estabelecida pelo art. 3º, § 5º, da Lei nº 8.666, de 1993.

## 4 OBRIGAÇÕES DA CONTRATADA

4.1 Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta;

4.2 Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

4.3 A CONTRATADA deverá oferecer atendimento por meio de Centro de Suporte Técnico, e deverá indicar telefone ou e-mail, devendo estar disponível para a abertura de chamados 24x7, inclusive feriados;

4.4 Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

4.5 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado ao Conselho Federal de Química ou à entidade federal, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

4.6 Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

4.7 Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária

4.8 Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010;

4.9 Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a empresa contratada deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a

regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT, conforme alínea "c" do item 10.2 do Anexo VIII-B da IN SEGES/MP n. 5/2017;

4.10 Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à Contratante;

4.11 Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

4.12 Prestar todo esclarecimento ou informação solicitada pela Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

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

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

4.15 Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado.

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

4.17 Submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo.

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

4.19 Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

4.20 Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social, bem como as regras de acessibilidade previstas na legislação, quando a contratada houver se beneficiado da preferência estabelecida pela Lei nº 13.146, de 2015.

4.21 Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

4.22 Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

4.23 Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante;

4.24 Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

4.25 Assegurar à CONTRATANTE, em conformidade com o previsto no subitem 6.1, “a” e “b”, do Anexo VII – F da Instrução Normativa SEGES/MP nº 5, de 25/05/2017:

4.25.1 O direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente, permitindo à Contratante distribuir, alterar e utilizar os mesmos sem limitações;

4.25.2 Os direitos autorais da solução, do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua utilização sem que exista autorização expressa da Contratante, sob pena de multa, sem prejuízo das sanções civis e penais cabíveis.

## 5 INSTRUMENTO DE MEDIÇÃO DE RESULTADO (IMR)

| **1) SERVIÇOS DE SUPORTE TÉCNICO, GARANTIA E MANUTENÇÃO** | |
|---|---|
| **ITEM** | **DESCRIÇÃO** |

| | |
|---|---|
| **FINALIDADE** | Solicitação formal de serviços de garantia/manutenção à contratada e devem ser atendidos de acordo com os critérios e parâmetros estabelecidos para execução dos serviços. |
| **META A CUMPRIR** | 6 Horas – Severidade Alta<br>12 Horas – Severidade Média<br>24 Horas – Severidade Baixa<br>Captura do chamado no sistema: até 1 hora<br><br>- Níveis de serviço<br><br>a) Alta– São emergências de falhas cujas consequências tenham impactos sobre o serviço e o tráfego e/ou recursos que exijam atenção imediata.<br><br>b) Média - São problemas graves ou falhas que afetam uma área específica ou determinada funcionalidade, porém não ocasiona a interrupção dos sistemas ou serviços.<br><br>c) Baixa - Problemas que não prejudiquem significativamente o funcionamento de sistemas ou serviços. |
| **INSTRUMENTO DE MEDIÇÃO** | Contador de tempo de chamado |
| **FORMA DE ACOMPANHAMENTO** | Pelo chamado |
| **PERIODICIDADE** | De acordo com a necessidade |
| **MECANISMO DE CÁLCULO** | A partir do horário de abertura e conclusão do chamado no sistema da contratada |
| **INÍCIO DE VIGÊNCIA** | Na data de assinatura do contrato |
| **SANSÕES** | **Severidade Alta**<br><br>***Até 2 (duas) horas corridas de atraso para solução do chamado****:*<br><br>- Advertência;<br>- Para as demais ocorrências, multa de 0,4% (quatro décimos por cento) por hora atrasada sobre o valor do contrato.<br><br>***Superior a 2 (duas) horas e inferior ou igual a 8 (oito) horas corridas de atraso para solução do chamado:***<br><br>- Multa de 0,6% (seis décimos por cento) por hora atrasada sobre o valor do contrato, sem prejuízo ao item anterior, e outras sanções administrativas a critério da CONTRATANTE, limitado a 15% do valor do contrato.<br><br>***Superior a 8 (oito) horas corridas para solução do chamado.***<br><br>- Multa de 0,8% (oito décimos por cento) por hora atrasada sobre o valor do contrato, sem prejuízo ao item anterior, e outras sanções administrativas a critério da CONTRATANTE, limitado a 15% do valor do contrato. |

| | |
|---|---|
| | **Severidade Média e Baixa**<br><br>**Até 8 (oito) horas corridas de atraso**,<br><br>- Advertência;<br>- Para as demais ocorrências, multa de 0,1% (um décimo por cento) por hora atrasada sobre o valor do contrato.<br><br>**Superior a 8 (oito) horas e inferior ou igual a 24 (vinte e quatro) horas corridas de atraso.**<br><br>- Multa de 0,2% (dois décimos por cento) por hora atrasada sobre o valor do contrato, sem prejuízo ao item anterior, e outras sanções administrativas a critério da CONTRATANTE, limitado a 15% do valor do contrato.<br><br>**Superior a 24 (vinte e quatro) horas corridas de atraso.**<br><br>- Multa de 0,3% (três décimos por cento) por hora atrasada sobre o valor do contrato, sem prejuízo ao item anterior, e outras sanções administrativas a critério da CONTRATANTE, limitado a 15% do valor do contrato. |

## 6 DA SUBCONTRATAÇÃO

6.1 Não será admitida a subcontratação do objeto licitatório.

## 7 ALTERAÇÃO SUBJETIVA

7.1 É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

## 8 CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

8.1 O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993.

8.2 O representante da Contratante deverá ter a qualificação necessária para o acompanhamento e controle da execução dos serviços e do contrato.

8.3 A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

8.4 A fiscalização do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a

adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º do artigo 65 da Lei nº 8.666, de 1993.

8.5 A conformidade do material/técnica/equipamento a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

8.6 O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993.

8.7 O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela Contratada ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 87 da Lei nº 8.666, de 1993.

8.8 As atividades de gestão e fiscalização da execução contratual devem ser realizadas de forma preventiva, rotineira e sistemática, podendo ser exercidas por servidores, equipe de fiscalização ou único servidor, desde que, no exercício dessas atribuições, fique assegurada a distinção dessas atividades e, em razão do volume de trabalho, não comprometa o desempenho de todas as ações relacionadas à Gestão do Contrato.

8.9 A fiscalização técnica dos contratos avaliará constantemente a execução do objeto e utilizará o Instrumento de Medição de Resultado (IMR).

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

8.11 Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

8.12 O fiscal técnico deverá apresentar ao preposto da CONTRATADA a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.

8.13 Em hipótese alguma, será admitido que a própria CONTRATADA materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

8.14 A CONTRATADA poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador.

8.15 Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, devem ser aplicadas as sanções à CONTRATADA de acordo com as regras previstas no ato convocatório.

8.16 O fiscal técnico poderá realizar avaliação diária, semanal ou mensal, desde que o período escolhido seja suficiente para avaliar ou, se for o caso, aferir o desempenho e qualidade da prestação dos serviços.

8.17 A conformidade do material a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da CONTRATADA que contenha sua relação detalhada, de acordo com o estabelecido neste Termo de Referência e na proposta, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

8.18 As disposições previstas nesta cláusula não excluem o disposto no Anexo VIII da Instrução Normativa SLTI/MP nº 05, de 2017, aplicável no que for pertinente à contratação.

8.19 A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

## 9 DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

9.1 Os equipamentos instalados deverão ser configurados de modo a garantir total interoperabilidade no ambiente computacional do Conselho Federal de Química e otimizados para usufruir das melhores condições em termos de desempenho, disponibilidade e segurança.

9.2 A CONTRATADA assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio do Conselho Federal de Química ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando da instalação e configuração da solução, na área de prestação dos serviços, mesmo que fora do exercício das atribuições previstas no contrato.

9.3 O recebimento da solução será feito em duas etapas:

9.3.1 Recebimento Provisório, até 5 (cinco) dias após a aprovação do projeto de instalação, na ocasião será expedido o termo de conformidade com modelo disponível no Anexo I.

9.3.2 Recebimento definitivo (Anexo II), até 15 (quinze) dias da instalação/configuração e a devida verificação, sendo confirmada sua operação e desempenho a contento, de acordo com os requisitos deste Termo e do Termo de Contrato. Toda a documentação de instalação física dos equipamentos, bem como os termos de garantia, também faz parte da aceitação definitiva. Na ocasião será expedido o Termo de Confidencialidade com modelo disponível no anexo III.

9.3.3 Conforme Art. 73, §2 da Lei n° 8.666/93 "***O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança da obra ou serviço, nem ético-profissional pela perfeita execução do contrato do contrato, dentro dos limites estabelecidos pela Lei ou pelo contrato***".

9.4 A CONTRATADA deverá entregar, às suas expensas, todos os itens acessórios de hardware necessários à perfeita instalação e funcionamento dos equipamentos, incluindo conectores, cabos, suportes e demais itens necessários para instalação e funcionamento da solução contratada, em plena compatibilidade com as especificações constantes neste Termo de Referência e recomendadas pelo fabricante.

9.5 Todos os equipamentos fornecidos e seus componentes deverão ser novos, de primeiro uso e devem estar acondicionados adequadamente em caixa lacrados de fábrica, de forma a propiciar completa segurança durante e transporte.

9.6 Constatada a ocorrência de divergência na especificação técnica, falhas de componentes, defeitos de fabricação e operação ou qualquer outro defeito apresentado durante o transporte, a entrega e a instalação dos equipamentos, fica a CONTRATADA obrigada a providenciar a substituição do equipamento, em até 5 (cinco) dias úteis, contatados a partir da notificação da ocorrência por parte da CONTRATANTE.

9.7 Eventuais despesas de custeio com deslocamento de técnicos da CONTRATADA ao local da instalação, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos ficam a cargo exclusivo da CONTRATADA.

9.8 A contratada deverá entregar toda a documentação de instalação física dos equipamentos, a qual deverá prover um nível de informação suficiente para que um técnico possa entender e refazer, caso necessário, as instalações e configuração.

**METODOLOGIA DE AVALIAÇÃO DA QUALIDADE**

| ID | ETAPA/FASE/ITEM | MÉTODO DE AVALIAÇÃO |
|---|---|---|
| 1 | Entrega dos Equipamentos | Conferência do equipamento entregue, comparando modelo com o especificado no contrato estabelecido entre o Conselho Federal de Química e a CONTRATADA. |
| 2 | Projeto de Instalação da Solução | Conferência dos itens mínimos do Projeto de Instalação da Solução. Elaboração do Termo de Aceite Provisório. |
| 3 | Instalação dos Equipamentos | Avaliação pela CONTRATANTE da montagem dos equipamentos feita pela CONTRATADA, com a respectiva verificação do funcionamento de todos os itens componentes da solução. |
| 4 | Configuração dos Equipamentos | Testes pela CONTRATADA das funcionalidades requisitadas no Contrato |
| 5 | Repasse de conhecimento. | Repasse de conhecimento de todo gerenciamento da solução, incluindo relatórios. |
| 6 | Aceite Final | Verificação final de instalação e configuração da solução e funcionalidades dos equipamentos. |

| | | |
|---|---|---|
| | | Elaboração do Termo de Aceite Definitivo. |

**PAGAMENTOS**

9.9 O pagamento será efetuado em sua totalidade (100%) do valor global contratado, assim que os produtos forem formalmente recebidos e em produção pelo CONTRATANTE, onde será emitido o Termo de Recebimento Definitivo.

9.10 O pagamento será efetuado até o 15° (décimo quinto) dia útil, contados do Termo de Recebimento definitivo.

9.11 A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

9.12 Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

9.12.1 O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

9.12.2 o prazo de validade;

9.12.3 a data da emissão;

9.12.4 os dados do contrato e do órgão contratante;

9.12.5 o período de prestação dos serviços;

9.12.6 o valor a pagar; e

9.12.7 eventual destaque do valor de retenções tributárias cabíveis.

9.13 Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;

9.14 Nos termos do item 1, do Anexo VIII-A da Instrução Normativa SEGES/MP nº 05, de 2017, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

9.14.1 não produziu os resultados acordados;

9.14.2 deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

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

9.15 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

9.16 Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

9.17 Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

9.18 Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

9.19 Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

9.20 Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

9.21 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

9.22 Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

9.23 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1993, nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.

9.24 É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante, com fundamento na Lei de Diretrizes Orçamentárias vigente.

9.25 Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX)^{\frac{(6/100)}{365}}$$

I = 0,00016438
TX = Percentual da taxa anual = 6%

**CRONOGRAMA DE EXECUÇÃO FÍSICA E FINANCEIRA**

| BENS/SERVIÇOS E OUTROS | DATA | RESPONSÁVEL | PERCENTUAL PAGO |
|---|---|---|---|
| Entrega dos Equipamentos | Até 60 (sessenta) dias corridos, após assinatura da ordem de serviço | CONTRATADA | 50% do valor dos equipamentos após a emissão do Termo de Recebimento Definitivo dos Equipamentos |
| Entrega do Projeto de Instalação | Até 10 (dez) dias corridos, após a entrega dos equipamentos | CONTRATADA | 0% |
| Aceite Provisório | Até 5 (cinco) dias após aprovação do projeto de instalação | CONTRATANTE | 0% |
| Instalação e Configuração | Até 15 (quinze) dias após o aceite provisório | CONTRATADA | 0% |
| Repasse de Conhecimento | Data a ser definida posteriormente | CONTRATADA | 0% |
| Aceite definitivo | Até 15 (quinze) dias da Instalação/configuração e a devida verificação. | CONTRATANTE | 50% do valor dos equipamentos e serviços prestados após a emissão do Termo de Recebimento Definitivo dos Equipamentos |

**10 GARANTIA DA EXECUÇÃO**

10.1 O adjudicatário prestará garantia de execução do contrato, nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e por 90 (noventa) dias após o término da licença de garantia do equipamento, em valor correspondente a 5% (cinco por cento) do valor total do contrato.

10.2 No prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do contratante, contados da assinatura do contrato, a contratada deverá apresentar comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

10.3 A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento).

10.4 O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n. 8.666 de 1993.

10.5 A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da licença de garantia.

10.6 A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

10.6.1 prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

10.6.2 prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

10.6.3 multas moratórias e punitivas aplicadas pela Administração à contratada; e

10.6.4 obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela contratada, quando couber.

10.7 A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

10.8 A garantia em dinheiro deverá ser efetuada em favor da Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

10.9 Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

10.10 No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

10.11 No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

10.12 Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

10.13 A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

10.14 Será considerada extinta a garantia:

10.14.1 com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

10.14.2 no prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h2"do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

10.15 O garantidor não é parte para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

10.16 A contratada autoriza a contratante a reter, a qualquer tempo, a garantia, na forma prevista no neste Edital e no Contrato.

## 11 DAS SANÇÕES ADMINISTRATIVAS

11.1 Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a CONTRATADA que:

11.1.1 inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

11.1.2 ensejar o retardamento da execução do objeto;

11.1.3 falhar ou fraudar na execução do contrato;

11.1.4 comportar-se de modo inidôneo; ou

11.1.5 cometer fraude fiscal.

11.2 Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

11.2.1 Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

11.2.2 Multa de:

11.2.2.1 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

11.2.2.2 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;

11.2.2.3 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

11.2.2.4 0,2% a 3,2% por dia sobre o valor mensal do contrato, conforme detalhamento constante das tabelas 1 e 2, abaixo; e

11.2.2.5 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

11.2.2.6 as penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

11.2.3 Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

11.2.3.1 Sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos.

11.2.3.2 Sansão de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 18.1 deste Termo de Referência.

11.2.4 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 Contratada ressarcir a Contratante pelos prejuízos causados;

11.2.5 As sanções previstas nos subitens 11.2.1, 11.2.3, 11.2.4 e 11.2.5 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

11.2.6 Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 1 e 2:

**Tabela 1**

| GRAU | CORRESPONDÊNCIA |
|---|---|
| 1 | 0,2% ao dia sobre o valor do contrato |
| 2 | 0,4% ao dia sobre o valo do contrato |
| 3 | 0,8% ao dia sobre o valor do contrato |
| 4 | 1,6% ao dia sobre o valor do contrato |
| 5 | 3,2% ao dia sobre o valor do contrato |

**Tabela 2**

| INFRAÇÃO | | |
|---|---|---|
| **ITEM** | **DESCRIÇÃO** | **GRAU** |
| 1 | Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais, por ocorrência; | 05 |
| 2 | Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia | 04 |

| | | |
|---|---|---|
| | e por unidade de atendimento; | |
| 3 | Manter funcionário sem qualificação para executar os serviços contratados, por empregado e por dia; | 03 |
| 4 | Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia; | 02 |
| 5 | Retirar funcionários ou encarregados do serviço durante o expediente, sem a anuência prévia do CONTRATANTE, por empregado e por dia; | 03 |
| **Para os itens a seguir, deixar de:** | | |
| 6 | Registrar e controlar, diariamente, a assiduidade e a pontualidade de seu pessoal, por funcionário e por dia; | 01 |
| 7 | Cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência; | 02 |
| 8 | Substituir empregado que se conduza de modo inconveniente ou não atenda às necessidades do serviço, por funcionário e por dia; | 01 |
| 9 | Cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência; | 03 |
| 10 | Indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato; | 01 |
| 11 | Providenciar treinamento para seus funcionários conforme previsto na relação de obrigações da CONTRATADA | 01 |

11.2.7 Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

11.2.7.1 tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

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

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

11.2.8 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

11.2.9 As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor do Conselho Federal de Química, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

11.2.9.1 Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

11.2.10 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, o Conselho Federal de Química ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

11.2.11 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.

11.2.12 Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

11.2.13 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

11.2.14 O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

11.2.15 As penalidades serão obrigatoriamente registradas no SICAF.

**CRITÉRIOS DE SELEÇÃO DO FORNECEDOR.**

12. As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no edital.

12.1 Os critérios de qualificação econômica a serem atendidos pelo fornecedor estão previstos no edital.

12.2 Os critérios de qualificação técnica a serem atendidos pelo fornecedor serão:

12.3 01 (um) ou mais atestado (s) / declaração (ões) de capacidade técnica, em nome da LICITANTE, expedido por pessoa jurídica de direito público ou privado, que comprove a aptidão para desempenho de atividade pertinente e compatível com o objeto licitado em características, quantidades e prazos de execução, devendo o atestado conter, além do nome do atestante, endereço e telefone da pessoa jurídica, ou qualquer forma de que o Conselho Federal de Química possa valer-se para manter contato com a empresa declarante.

12.4 O Conselho Federal de Química se resguarda no direito de diligenciar junto à pessoa jurídica emitente do Atestado/Declaração de Capacidade Técnica, visando obter informações sobre o fornecimento dos produtos, serviços e cópias dos respectivos contratos e/ou outros documentos comprobatórios do conteúdo declarado.

12.5 Os critérios de aceitabilidade de preços serão:

12.6 O critério de julgamento da proposta é o menor preço global.

12.7 As regras de desempate entre propostas são as discriminadas no edital.

**ESTIMATIVA DE PREÇOS E PREÇOS REFERENCIAIS.**

13.1 O custo estimado da contratação é de R$ 79.466,21 (setenta e nove mil, quatrocentos e sessenta e seis reais e vinte e um centavos).

**DOS RECURSOS ORÇAMENTÁRIOS.**

14.1 A aquisição está prevista no projeto “Infraestrutura de TIC”, nas seguintes contas orçamentárias:

- Centro de custo 02.08.03.501 (Projeto Infraestrutura de TIC) e conta contábil 6.2.2.1.2.44.90.52.004 (Equipamentos de Informática);
- Centro de Custo 02.08.03.501(Projeto Infraestrutura de TIC) e conta contábil 6.2.2.1.33.90.39.025 (Serviços de Seleção, Treinamento e Aperfeiçoamento);
- Centro de Custo 02.08.03.501 (Projeto Infraestrutura de TIC) e conta contábil 6.2.2.1.33.90.39.056 (Serviços de Informática – Redes e Suporte);

- Centro de Custo 02.08.03.501 (Projeto Infraestrutura de TIC) e conta contábil 6.2.2.1.33.90.39.006 (Licença de Uso de Sistemas de Informática – Software);

Este Termo de Referência foi elaborado conforme o inciso I do art. 14º do Decreto 10.024/2019, por:

| | |
|---|---|
| Eurípedes Alexandre Rocha | Sebastião Diego da Conceição Santos |
| **INTEGRANTE TÉCNICO** | **INTEGRANTE ADMINISTRATIVO** |

Cristiano Xavier Lucas Ferreira
**INTEGRANTE REQUISITANTE**

Aprovo este Termo de Referência conforme o inciso II do art. 14º do Decreto nº 10.024/2019:

Brasília/DF, 18 de junho de 2020.

**José de Ribamar Oliveira Filho**
Presidente do CFQ