Conselho Federal de Química

Plenário
Presidência
Gerência Executiva
Gerência de Tecnologia da Informação e Comunicação

ESTUDO TÉCNICO PRELIMINAR: TI

Processo nº 2800.00.04327.2024

Aquisição de solução de firewall e serviço de suporte técnico especializado em TIC.

Referência: Art. 11 da IN nº 94/2022.

Histórico de Revisões

Data	Versão	Descrição	Autor
09/01/2025	1.0	Finalização da primeira versão do documento	Renato Araújo Santana
13/02/2025	1.1	Revisão e ajustes	Renato Araújo Santana e Aline Medeiros
21/02/2025	1.2	Revisão e ajustes	Deborah Alencar
12/03/2025	1.3	Revisão e ajustes	Renato Araújo Santana
21/03/2025	1.4	Revisão e ajustes	Viviane Glaucia Souza
25/03/2025	2.0	Finalização da segunda versão do documento	Renato Araújo Santana
29/03/2025	2.1	Revisão e ajustes	Viviane Glaucia Souza
07/05/2025	2.2	Revisão e ajustes	Renato Araújo Santana
12/06/2025	2.3	Ajustado após análise jurídica	Renato Araújo Santana

1. INTRODUÇÃO

1.1. Este estudo técnico preliminar tem como objetivo identificar a necessidade e justificar a aquisição de solução de firewall para o Conselho Federal de Química.

2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

2.1. O Conselho Federal de Química (CFQ), instituído pela Lei nº 2.800, de 18 de junho de 1956, é uma autarquia federal responsável por promover o pleno desenvolvimento da atividade química, com foco no fomento ao crescimento sustentável do país. Para o cumprimento de sua missão institucional, o CFQ conta com uma estrutura organizacional composta pela presidência, conselheiros, gerências executivas e áreas técnicas e administrativas.

2.2. A Tecnologia da Informação e Comunicação (TIC) é um recurso fundamental para o bom funcionamento das organizações públicas, sendo imprescindível para que o CFQ cumpra suas funções e objetivos institucionais. A TIC não só proporciona a interligação de sistemas e dados, mas também apoia na melhoria contínua dos processos administrativos e operacionais.

2.3. A Gerência de Tecnologia da Informação (GETIC) tem como responsabilidade o desenvolvimento e a implementação de soluções tecnológicas que atendam aos seguintes objetivos estratégicos do CFQ:

I - OE15 Adotar um sistema integrado e inovador de informações, capaz de

interligar o sistema CFQ/CRQs e as partes interessadas.

II - OE12: Promover a inovação de processos e serviços por meio da melhoria contínua e do uso de ferramentas de Inteligência Artificial.

2.4. A infraestrutura de TIC do CFQ é composta por uma série de ativos agrupados nas áreas de segurança da informação, redes de comunicação de voz e dados, bancos de dados, servidores de rede, sistemas operacionais, sistemas de backup e armazenamento de dados. Estes recursos são essenciais para o desempenho das atividades do CFQ, sendo que qualquer falha ou interrupção nos serviços de TIC pode comprometer seriamente a continuidade das operações do órgão e afetar negativamente sua capacidade de atingir seus objetivos institucionais.

2.5. A contratação de uma solução de firewall, especialmente Next-Generation Firewall (NGFW), é essencial para proteger o ambiente digital da organização contra ameaças cibernéticas cada vez mais sofisticadas. Além de monitorar e controlar o tráfego da rede, essa tecnologia oferece recursos avançados, como detecção de intrusões, prevenção de ataques e inspeção profunda de pacotes. Ao implementar uma solução de firewall em ambiente de alta disponibilidade (HA), garante-se não apenas a segurança proativa, mas também a continuidade dos serviços, minimizando riscos operacionais e assegurando a conformidade com normas de proteção de dados.

2.6. A solução de firewall atualmente em utilização no Conselho Federal de Química tem prazo de fim de vida útil (End of Life) definido pelo fabricante para a data de 31/03/2025. Diante desse cenário, é necessária a contratação de nova aplicação de firewall para o CFQ. O projeto deve considerar a futura mudança de local da sede do CFQ para a sede SAUS, em data ainda a ser definida, e a alta disponibilidade do serviço, visando a continuidade de todas as atividades internas e externas deste Conselho.

2.7. O NGFW é recomendado para proteção de informação perimetral e de rede interna que inclui statefull firewall com capacidade para para controle de tráfego de dados por identificação de usuários e por camada 7 (aplicação), 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 e-mail, inspeção de tráfego criptografado e proteção de firewall de aplicação Web.

2.8. Sendo assim, a contratação da solução de firewall engloba:

Grupo	Descrição	CATMAT	Quantidade
Único	Appliance [1] *Firewall Next-Generation em ambiente de alta disponibilidade (HA), licença de uso, fonte redundante, instalação, treinamento e suporte técnico durante a vigência do contrato.*	609340	2

2.9. O objeto da licitação enquadra-se na categoria de bem comum, por possuir padrões de desempenho e características gerais e específicas, 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.

2.10. O quantitativo e respectivo código do item estão discriminados na tabela acima.

2.11. A presente contratação está alinhada aos seguintes objetivos estratégicos de TIC:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
ID	**Objetivos Estratégicos**	**Nome do documento e vigência**
OE 12	Promover a inovação de processos e serviços, por meio da melhoria contínua e das ferramentas de Inteligência Artificial.	- PPA 2025 - 2027 - Eixo 1 | Transformação Digital e Inovação; -Planejamento Estratégico do Sistema CFQ/CRQ-2018; -Mapa Estratégico / 2018 – 2028; -Plano Diretor de Tecnologia da Informação PDTIC 2025-2027.

ALINHAMENTO AO PDTIC 2025-2027		
ID	**Ação do PDTIC**	**Meta do PDTIC associada**
A01	Aquisição de solução de Firewall	Indicador: Contratação Realizada /Contratação Planejada Metas: 2° TRI/2024: 60% 3° TRI/2024: 40%

IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS	
A01 - Aquisição de solução de Firewall.	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. 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.

2.12. **Requisitos de Negócio**

2.12.1. O desempenho das atividades do Conselho Federal de Química depende de uma infraestrutura de TIC eficiente, que inclui equipamentos, softwares, servidores, conectividade à internet, rede de comunicação e outros serviços essenciais.

2.12.2. Para garantir o correto funcionamento da rede de dados, o CFQ precisa de ferramentas e equipamentos que garantam sua disponibilidade, bem como a proteção de entrada na rede, evitando assim riscos associados à tecnologia da informação, como vírus e ransomware.

2.12.3. Com o crescimento da demanda por recursos tecnológicos, a infraestrutura de TIC deve sustentar o desenvolvimento da missão do CFQ e contribuir para sua visão de "Ser reconhecido como referência no desenvolvimento da Química no Brasil".

2.12.4. A solução de TIC contratada deverá garantir a eficiência, produtividade, confiabilidade e disponibilidade dos serviços, incluindo:

a) Garantir a proteção de dados sensíveis da organização contra ataques cibernéticos;

b) Cumprir com requisitos legais e regulatórios, como a **LGPD** (Lei Geral de Proteção de Dados) e outras normas aplicáveis;

c) Prevenir acesso não autorizado à rede interna;

d) Minimizar interrupções nos serviços causadas por incidentes de segurança;

e) Implementar alta disponibilidade e redundância na solução de firewall para assegurar operação contínua;

f) Possuir capacidade de escalabilidade para atender ao crescimento da organização;

g) Controle granular de acesso para usuários internos e externos com base em funções,

departamentos ou perfis;

h) Implementação de inspeção de tráfego criptografado (SSL/TLS) sem prejudicar o desempenho;

i) Monitorar o tráfego em tempo real e gerar alertas para eventos críticos;

j) Disponibilizar relatórios detalhados para análise de segurança, incluindo detecção de anomalias e auditorias;

k) Oferecer integração com sistemas SIEM (Gerenciamento de Eventos e Informações de Segurança);

l) Interface de administração amigável para configuração e monitoramento;

m)Capacidade de gerenciar múltiplas filiais ou escritórios de forma centralizada;

n) Atualizações automáticas de firmware e assinaturas de segurança;

o) Suportar o volume de tráfego atual e oferecer escalabilidade para expansão futura;

p) Garantir baixa latência e alto desempenho mesmo com múltiplas funcionalidades habilitadas (como inspeção de conteúdo e antivírus integrado);

q) Oferecer treinamento para a equipe interna de TIC, garantindo autonomia no gerenciamento; e

r) Garantir suporte contínuo para atualizações e patches de segurança.

2.12.5. A contratação do serviço deverá estar alinhada às melhores práticas do mercado e às exigências do setor público, garantindo a efetividade e a segurança nos processos de TIC.

2.12.6. 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 durante a vigência do contrato.

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

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

2.12.9. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico. A solução deverá contemplar a totalidade das capacidades exigidas, sendo permitido o uso de um equipamento para a solução.

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

2.12.11. 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.

2.13. **Requisitos Legais**

2.13.1. A contratação objeto deste Estudo Técnico Preliminar - ETP tem amparo legal nos seguintes dispositivos legais:

a) Instrução Normativa SGD/ME Nº 94, de 23 de dezembro de 2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação – TIC pelos órgãos e entidades integrantes do Sistema de Administração dos recursos de Tecnologia da Informação – SISP do Poder Executivo Federal.

b) Lei nº 12.846, de 01 de agosto de 2013, que estabelece a responsabilização administrativa e civil de pessoas jurídicas pela prática contra a administração pública, nacional e estrangeira.

c) Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD): A prestação de serviços ao CFQ deverá estar alinhada à legislação brasileira no que se refere ao tratamento dos dados deste Conselho.

d) Lei nº 14.133, de 1° de abril de 2021, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios.

2.14. **Requisitos de Capacitação**

2.14.1. Considerando as tecnologias utilizadas no ambiente de TIC do CFQ, a empresa contratada deverá contar com uma equipe técnica especializada, com treinamento e capacitação atualizados nas tecnologias pertinentes, que levem em consideração o parque tecnológico do CFQ.

2.14.2. Os requisitos de capacitação devem abranger as principais metodologias, tecnologias, produtos e ferramentas relacionadas aos serviços de TIC e infraestrutura utilizados pelo CFQ, garantindo a expertise necessária para a execução do contrato.

2.14.3. A capacitação contínua é essencial para mitigar riscos de falhas na prestação dos serviços, assegurando a disponibilidade e a qualidade dos serviços de TIC para os usuários e para a sociedade.

2.14.4. Os requisitos de capacitação não se limitam apenas aos aspectos mencionados.

2.15. **Requisitos de gerenciamento, monitoramento e suporte técnico**

2.15.1. A aplicação deverá monitorar a rede do CFQ no modelo 24x7, podendo a equipe de TIC do CFQ intervir e fazer as devidas correções, quando necessário e oportuno.

2.15.2. No caso da ocorrência de incidentes que comprometam a rede de dados do CFQ, a equipe de TIC do CFQ deverá receber o suporte necessário para que possa agir prontamente para identificar, mitigar, prevenir e solucionar as ocorrências.

2.15.3. Os atendimentos de suporte técnico devem ser providos pela CONTRATADA em dias úteis, no período de 8h as 18h.

2.15.4. O atendimento será preferencialmente remoto. Caso haja necessidade de intervenção local, esta poderá ser executada em acordo com a CONTRATANTE. Nos dois casos, sempre com acompanhamento pela equipe técnica da CONTRATANTE.

2.16. **Requisitos de Segurança**

2.16.1. A contratada deverá assinar Termo de Compromisso de Manutenção de Sigilo e os respectivos funcionários alocados ao projeto deverão assinar o Termo de Ciência.

2.16.2. A contratada deverá apresentar, na reunião inicial, relação nominal dos profissionais envolvidos na execução do contrato que deverão ter acesso às informações do CFQ, quando necessário, bem como os referidos Termos assinados. Caberá ao preposto alocado ao contrato manter esta lista atualizada sempre que um novo profissional necessitar de acesso às informações do CFQ.

2.16.3. A CONTRATADA deverá cumprir a Política de Segurança da Informação da CONTRATANTE e assumir responsabilidade sobre todos os possíveis danos físicos e/ou materiais causados à CONTRATANTE, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança.

2.16.4. A CONTRATADA não poderá veicular publicidade acerca dos serviços contratados, sem prévia e formal autorização por parte da CONTRATANTE.

2.16.5. É vedado à CONTRATADA o acesso aos dados da CONTRATANTE, sem prévia e formal autorização por parte da CONTRATANTE.

2.16.6. As informações sob custódia do fornecedor deverão ser tratadas como informações sigilosas, não podendo ser usadas por este fornecedor ou fornecidas, sob nenhuma hipótese, sem autorização formal da CONTRATANTE.

2.16.7. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CFQ, possibilitará a imediata rescisão de contrato firmado entre o CFQ e a contratada, sem qualquer ônus para o CFQ, ensejando reparação por perdas e danos sofridos pelo CFQ,

inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas.

2.16.8. A CONTRATADA deve comunicar formal e imediatamente à CONTRATANTE qualquer ponto de fragilidade percebido que exponha a confidencialidade, integridade ou disponibilidade das informações e do serviço.

2.17. **Requisitos Técnicos e de Arquitetura Tecnológica**

2.17.1. Características específicas de hardware considerando Firewalls do tipo Next Generation:

2.17.2. Deve suportar, no mínimo, 25 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, considerando pacotes de 512 bytes;

2.17.3. Deve suportar, no mínimo, 3 Gbps de throughput IPS.

2.17.4. Deve suportar, no mínimo, 20 Gbps de throughput de VPN IPSec.

2.17.5. Deve suportar, no mínimo, 1 Gbps de throughput de VPN SSL.

2.17.6. Deve suportar, no mínimo, 2 Gbps de throughput de Inspeção SSL.

2.17.7. Deve suportar, no mínimo, 5 Gbps de throughput de Controle de Aplicação.

2.17.8. Deve suportar, no mínimo, 2 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware.

2.17.9. Suporte a, no mínimo, 1 milhões de conexões simultâneas;

2.17.10. Deve suportar o gerenciamento de no mínimo 20 Pontos de Acesso Wi-Fi do mesmo fabricante em modo Tunel, ou até 100 em modo “Bridge”, com saída local na unidade;

2.17.11. Deve suportar o gerenciamento de no mínimo 15 Switches do mesmo fabricante por equipamento;

2.17.12. Suporte a, no mínimo, 100 mil novas conexões por segundo;

2.17.13. Estar licenciado para, ou suportar sem o uso de licença, 1.500 túneis de VPN IPSEC Site-to-Site simultâneos;

2.17.14. Estar licenciado para, ou suportar sem o uso de licença, 15.000 túneis de clientes VPN IPSEC simultâneos;

2.17.15. Estar licenciado para, ou suportar sem o uso de licença, 500 clientes de VPN SSL simultâneos;

2.17.16. Caso seja necessário fornecimento de licenças para prover o uso de VPN para a quantidade de usuários solicitada, a licença deverá operar em caráter perpétuo;

2.17.17. Possuir ao menos 8 interfaces 1Gbps RJ-45;

2.17.18. Possuir ao menos 4 interfaces 1Gbps SFP;

2.17.19. Possuir ao menos 2 interfaces 10Gbps SFP+;

2.17.20. Deverá possuir interface USB 3.0 para exportação de backups;

2.17.21. Deverá possuir interface do tipo console para utilização de CLI;

2.17.22. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;

2.17.23. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;

2.17.24. Possuir no máximo 1 RU de altura;

2.17.25. Deverá ser fornecido com fonte de alimentação interna redundante;

2.18. **Requisitos de Projeto e de Implementação**

2.18.1. A solução deverá ser fornecida como appliance dedicado, não sendo aceitos equipamentos de propósito genérico (como PCs ou servidores) sobre os quais seria possível instalar sistemas operacionais convencionais (Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X, GNU/Linux). A

solução poderá ser entregue em equipamento único ou composta por um conjunto de dispositivos que atendam às funcionalidades exigidas.

2.18.2. A solução deverá prover proteção de informação perimetral e de rede interna que inclui recurso stateful 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 e-mail, inspeção de tráfego criptografado e proteção de aplicação Web.

2.18.3. A solução deverá fornecer console de gerenciamento dos equipamentos e centralização de logs em hardware específico ou virtualizado ou em plataforma própria.

2.18.4. A solução deverá ser ativada e licenciada com as seguintes funcionalidades: Roteamento, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, WAF Protection, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações e Otimização WAN.

2.18.5. A solução deverá possuir processadores dedicados e para fins específicos, desenvolvidos exclusivamente pelo fabricante da solução, com a finalidade de processar tráfegos de redes e acelerar o processamento destes pacotes de redes, mantendo a performance da solução sem comprometimento durante a execução de múltiplas funções de segurança simultaneamente.

2.18.6. O projeto de instalação e configuração deverá contemplar um plano de migração conforme a seguir:

2.18.6.1. Para garantir a segurança e a continuidade das operações, o projeto de implementação do novo firewall deve incluir um plano de migração detalhado das regras existentes, contemplando as seguintes diretrizes:

a) **Mapeamento e Migração**: Todas as regras atualmente configuradas no firewall em uso devem ser identificadas, documentadas e migradas para a nova solução, garantindo equivalência funcional e alinhamento com as políticas de segurança da organização;

b) **Testes e Validação** : Após a migração, todas as regras devem ser submetidas a um rigoroso processo de testes para assegurar sua eficácia e evitar impactos indesejados na operação da rede;

c) **Plano de Implementação**: A migração das regras não poderá ser realizada durante o expediente regular. Para isso, deve ser elaborado um cronograma de execução, prevendo janelas de manutenção fora do horário comercial. O plano deve ser submetido para aprovação da equipe técnica do CFQ, incluindo a definição de datas e etapas; e

d) **Plano de Contingência**: Deve ser estruturada uma estratégia de rollback para mitigar riscos e possibilitar a reversão rápida caso ocorra qualquer falha crítica na implementação.

2.18.6.2. Este requisito deve ser obrigatoriamente seguido para garantir a transição segura e eficiente para o novo firewall, minimizando impactos e assegurando a integridade da infraestrutura de TI.

2.18.7. Cada unidade de appliance deverá possuir, no mínimo, 02 (duas) fontes redundantes.

2.18.8. A solução deverá ser obrigatoriamente ser fornecida com equipamentos voltados para operação em modo de alta disponibilidade e estar licenciados para operar desta forma, os custos devem ser considerados na proposta inicial para solução em cluster.

2.18.9. A solução deverá licença para número ilimitado de usuários e endereços IP.

2.18.10. A solução deverá possuir licença capaz de permitir atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de proteção avançada durante a vigência contratual.

2.18.11. A solução deverá ser capaz de gerenciar, via funcionalidade de gestão Wireless, controlando Pontos de Acesso sem fio WIFI.

2.18.12. A solução deverá estar licenciada para permitir número ilimitado de estações de rede e usuários.

2.18.13. A solução deverá incluir licença para a funcionalidade de VPN SSL sem custos.

2.18.14. A solução deverá incluir licença para atualização de vacina de ameaças/anti-spyware.

2.18.15. A solução deverá incluir licença de atualização para filtro de conteúdo Web.

2.18.16. A solução deverá incluir licença de atualização do IPS e da lista de aplicações detectadas.

2.18.17. A solução deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

2.18.18. A solução deverá possuir controle de acesso à internet por endereço IP de origem e destino.

2.18.19. A solução deverá possuir controle de acesso à internet por sub-rede.

2.18.20. A solução deverá possuir ferramenta de diagnóstico do tipo tcpdump ou funcionalidade similar.

2.18.21. A solução deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory.

2.18.22. A solução deverá possuir recurso de DNS seguro, no qual as consultas são realizadas por meio de endereços seguros informados pelo próprio fabricante, no qual já possuir recurso integrado capaz de evitar ameaças.

2.18.23. A solução deverá suportar single-sign-on para Active Directory, Azure AD, eDirectory e RADIUS.

2.18.24. A solução deverá possuir métodos de autenticação de usuários que operem sob os protocolos TCP/IP.

2.18.25. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) no próprio software.

2.18.26. A solução deverá permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana.

2.18.27. A solução deverá permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br.

2.18.28. A solução deverá permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego.

2.18.29. A solução deverá suportar PBR – Policy Based Routing.

2.18.30. A solução deverá permitir a criação de VLANS no padrão IEEE 802.1q.

2.18.31. A solução deverá permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2.

2.18.32. A solução deverá suportar operações em multicast.

2.18.33. A solução deverá suportar roteamento multicast PIM Sparse Mode (SM).

2.18.34. A solução deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP.

2.18.35. A solução deverá permitir o agrupamento de serviços.

2.18.36. A solução deverá permitir o filtro de pacotes sem a utilização de NAT.

2.18.37. A solução deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas.

2.18.38. A solução deverá possuir mecanismo de anti-spoofing ou outro similar contra adulteração ou clonagem de MAC.

2.18.39. A solução deverá permitir criação de regras definidas pelo usuário.

2.18.40. A solução deverá permitir o serviço de autenticação para tráfego HTTP e FTP.

2.18.41. A solução deverá possuir a funcionalidade de balanceamento e contingência de links utilizando de configurações para balanceamento ou redundância ou ambos os casos.

2.18.42. A solução deverá ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar.

2.18.43. A solução deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS.

2.18.44. A solução deverá permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.

2.18.45. A solução deverá permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras.

2.18.46. A solução deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

2.18.47. A solução deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web: Proxy anônimo; Webmail; Instituições de saúde; Notícias; Phishing; Hackers; Pornografia; Racismo; Websites pessoais; Compras.

2.18.48. A solução deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

2.18.49. A solução deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.

2.18.50. A solução deverá prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado.

2.18.51. A solução deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.

2.18.52. A solução deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.

2.18.53. A solução deverá ser capaz de realizar análise do ambiente existente com o levantamento da infraestrutura de rede atual, incluindo topologia, dispositivos existentes e requisitos de compatibilidade.

2.18.54. A solução deverá permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.

2.18.55. A solução deverá estar orientada à proteção de redes.

2.18.56. A solução deverá permitir funcionar em modo transparente, sniffer e router.

2.18.57. A solução deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

2.18.58. A solução deverá permitir a criação de padrões de ataque manualmente;

2.18.59. A solução deverá possuir integração à plataforma de segurança;

2.18.60. A solução deverá possuir capacidade de remontagem de pacotes para identificação de ataques;

2.18.61. A solução deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;

2.18.62. A solução deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

2.18.63. A solução deverá possuir mecanismos de detecção/proteção de ataques;

2.18.64. A solução deverá possuir reconhecimento de padrões;

2.18.65. A solução deverá possuir análise de protocolos;

2.18.66. A solução deverá possuir detecção de anomalias;

2.18.67. A solução deverá possuir detecção de ataques de RPC (Remote Procedure Call);

2.18.68. A solução deverá possuir proteção contra-ataques de Windows ou NetBios;

2.18.69. A solução deverá possuir proteção contra-ataques DNS (Domain Name System);

2.18.70. A solução deverá possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;

2.18.71. A solução deverá possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);

2.18.72. A solução deverá possuir métodos de notificação de detecção de ataques;

2.18.73. A solução deverá possuir alarmes na console de administração;

2.18.74. A solução deverá possuir alertas via correio eletrônico;

2.18.75. A solução deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

2.18.76. A solução deverá ter a capacidade de resposta/logs ativa a ataques;

2.18.77. A solução deverá prover a terminação de sessões via TCP resets;

2.18.78. A solução deverá armazenar os logs de sessões;

2.18.79. A solução deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

2.18.80. A solução deverá mitigar os efeitos dos ataques de negação de serviços;

2.18.81. A solução deverá permitir a criação de assinaturas personalizadas;

2.18.82. A solução deverá possuir filtros de ataques por anomalias;

2.18.83. A solução deverá suportar mitigar ataques de DoS, com limite de sessão;

2.18.84. A solução deverá suportar verificação de ataque na camada de aplicação;

2.18.85. A solução deverá suportar verificação de tráfego em tempo real, via aceleração de hardware;

2.18.86. A solução deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset.

2.18.87. A solução deverá ter como configuração básica do sistema:

a) Definição de endereços IP para interfaces de rede;

b) Configuração de rotas estáticas e gateways;

c) Ajustes de data, hora e sincronização com NTP;

d) Configuração de alta disponibilidade (HA): Implementação de redundância (ativo-ativo ou ativo-passivo) para garantir continuidade;

e) Políticas de acesso: Criação e validação de regras de controle de acesso baseadas em usuários, grupos e localizações;

f) Configuração de inspeção de tráfego: Ativação de inspeção profunda de pacotes (DPI) e proteção contra ameaças;

g) Configuração de filtros web: Ativação de políticas de filtragem de conteúdo (web filtering) para bloquear acesso a sites e categorias não autorizadas;

h) Teste de HA: Garantir que a alta disponibilidade funcione corretamente em caso de falha de um dos dispositivos;

i) Treinamento operacional: Fornecimento de treinamento para os administradores sobre como gerenciar e monitorar o firewall;

j) Transferência de conhecimento: Explicação das configurações implementadas e boas práticas de administração;

k) Documentação técnica: Entrega de documentação completa das configurações realizadas, incluindo diagramas e políticas implementadas;

l) Período de acompanhamento: Disponibilidade para correções e ajustes após a instalação, durante um período acordado;

m)Atualizações iniciais: Aplicação de atualizações de firmware e assinaturas de segurança antes da entrega do ambiente;

n) SLA para suporte: Estabelecimento de um SLA para suporte técnico e resolução de problemas críticos após a instalação;

o) Validação final: Reunião para apresentar os resultados e verificar se todos os requisitos foram atendidos; e

p) Checklist de entregáveis: Confirmação de que os itens previstos no escopo foram entregues, como relatórios, documentação e acesso às configurações.

2.18.88. A contratada deverá :

a) Apresentar Documentação inicial: Registro do escopo, objetivos e pré-requisitos da instalação, acompanhado de Plano de implementação com a definição de etapas do projeto, cronograma e alocação de responsabilidades entre a equipe contratada e a equipe interna, incluindo a avaliação de possíveis impactos durante a instalação (ex.: interrupções de serviço) e estratégias para mitigá-los;

b) Instalar o equipamento no ambiente físico, incluindo racks, cabos e fontes de alimentação;

c) Configurar as portas físicas e conectividade entre o firewall e outros dispositivos da rede (switches, roteadores, etc.); e

d) Realizar teste de alimentação e inicialização: Verificação do funcionamento básico do equipamento (power-on self-test).

2.19. **FUNCIONALIDADE DE VPN**

2.19.1. A solução deverá possuir algoritmos de criptografia para túneis: AES, DES, 3DES.

2.19.2. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs.

2.19.3. A solução deverá possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-toSite.

2.19.4. A solução deverá possuir suporte a VPN SSL.

2.19.5. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais.

2.19.6. A solução deverá possuir acesso a VPN SSL deverá possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança.

2.19.7. A solução deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN.

2.19.8. A solução deverá suportar os protocolos L2TP, PPTP, VPN SSL, IPSEC.

2.19.9. A solução deverá proporcionar através do portal do usuário uma forma de conexão via HTML5 de acesso remoto com suporte aos protocolos, RDP, HTTP, HTTPS, SSH, Telnet e VNC.

2.19.10. A solução deverá suportar autenticação via AD/LDAP, Token e base de usuários local.

2.20. **FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES**

2.20.1. A solução deverá possuir categoria pré-definidas, como alguns exemplos de tipos de aplicações, como P2P; Instant Messaging; Web; Transferência de arquivos; VoIP.

2.20.2. A solução deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.

2.20.3. A solução deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.

2.20.4. A solução deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.

2.20.5. A solução deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.

2.20.6. A solução deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.

2.20.7. A solução deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.

2.20.8. A solução deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem.

2.20.9. A solução deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.

2.20.10. A solução deverá permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias exemplos: Instant Messaging e transferência de arquivos.

2.20.11. A solução deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

2.20.12. A solução deverá possuir logs e relatórios que informem todos eventos de APT.

2.20.13. A solução deverá permitir que o administrador possa configurar entre apenas logar os eventos ou logar e bloquear as conexões consideradas ameaças persistentes.

2.20.14. A solução deverá em casos de falso positivo, permitir ao administrador criar exceções para o fluxo considerado como APT.

2.21. **FUNCIONALIDADE DE BALANCEAMENTO DE CARGA**

2.21.1. A solução deverá permitir a criação de endereços IPs virtuais ou aliás.

2.21.2. A solução deverá suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP.

2.21.3. A solução deverá permitir balanceamento, ao menos, com os seguintes métodos: session persistence e Round Robin.

2.21.4. A solução deverá permitir persistência de sessão.

2.21.5. A solução deverá permitir que seja mantido o IP de origem.

2.21.6. A solução deverá a solução deverá suportar offloading em seus equipamentos.

2.21.7. A solução deverá ter a capacidade de identificar, através de health checks, quais os links que estejam ativos, removendo automaticamente o link que não esteja operacional.

2.21.8. A solução deverá permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP com o endereço IP.

2.22. **FUNCIONALIDADE DE SD-WAN**

2.22.1. A solução SD-WAN deverá ser viabilizada com recursos de segurança integrados de: Navegação, VPN, Antivírus, IPS e Filtro de Segurança Web.

2.22.2. A solução SD-WAN deverá suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

2.22.3. A solução SD-WAN deverá suportar micro-segmentação de tráfego onde seja possível aplicar políticas de navegação entre segmentos de LAN.

2.22.4. A solução SD-WAN deverá prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

2.22.5. A solução deverá ser capaz de prover Zero Touch provisioning.

2.22.6. A solução de Zero Touch provisioning deve ser capaz de facilitar as implantações.

2.22.7. A solução deverá ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz ou seja realizar redundância de acessos.

2.22.8. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados.

2.22.9. A solução de SD-WAN deve suportar configuração com suporte a IPv6.

2.22.10. A solução deverá ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD- WAN em condições pré-definidas forem modificadas.

2.22.11. A solução deverá ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

2.22.12. A solução deverá permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.

2.23. **GARANTIA, SUPORTE E LICENCIAMENTO**

2.23.1. O licenciamento para todos os serviços de segurança, incluindo atualização dos equipamentos, coberturas em caso de falha de hardware(trocas), suporte do fabricante (abertura de ticket), atualizações de softwares, todos esses recursos devem ser cobertos durante a cobertura das licenças;

2.23.2. A garantia de hardware deverá diretamente com a fabricante, conforme prazo estabelecido neste termo;

2.23.3. A solução deverá contemplar suporte do Fabricante pelo período vigente, com no mínimo, as seguintes características:

2.23.4. O suporte do fabricante deverá ter um sistema de abertura de chamados para acompanhamento – funcionando 24 horas por dia e 7 dias por semana. O atendimento telefônico deverá operar em língua Portuguesa pelo menos em regime 8x5.

2.23.5. Deverá ser assegurada a utilização de novas versões de software da solução sem ônus a contratada, sempre que esta estiver disponível a qualquer cliente durante o prazo das licenças.

2.23.6. Deverá ser permitido o acesso à base de conhecimento da solução.

2.24. A presente contratação tem por objetivo suprir a necessidade de proteção avançada da infraestrutura tecnológica do Conselho Federal de Química (CFQ), por meio da aquisição de um **firewall de próxima geração** (Next-Generation Firewall – NGFW). Trata-se de uma medida essencial à manutenção da segurança, disponibilidade e integridade das informações institucionais, bem como à continuidade dos serviços prestados ao cidadão e à sociedade.

2.25. Do ponto de vista do interesse público, a contratação visa assegurar:

- **A proteção de dados sensíveis e estratégicos** sob a guarda da autarquia, em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018);
- **A continuidade dos serviços públicos digitais** essenciais à atuação reguladora e fiscalizatória do CFQ, reduzindo o risco de paralisações causadas por incidentes de segurança;
- **A conformidade com diretrizes de governança e gestão de riscos de TIC**, previstas em normativos da Administração Pública Federal, como o Decreto nº 10.332/2020 (Estratégia de Governo Digital) e as recomendações do TCU;
- **A otimização da gestão da segurança da informação**, por meio de recursos modernos de controle de tráfego, detecção de ameaças, segmentação de rede e resposta a incidentes.

2.26. Dessa forma, a contratação do firewall não apenas corrige uma lacuna técnica relevante, mas também responde diretamente ao interesse público na medida em que garante a continuidade e a segurança dos serviços prestados pela autarquia, contribuindo para a confiança institucional e a proteção

do cidadão no ambiente digital.

3. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

3.1. Em conformidade com o disposto no art. 11, incisos V e VI, da Instrução Normativa SEGES/ME nº 94/2022, apresentam-se a seguir as justificativas relativas à estimativa das **quantidades da contratação**.

3.2. **Estimativa das Quantidades a Serem Contratadas:** A presente contratação refere-se ao fornecimento de **02 (dois) appliances de firewall do tipo Next-Generation (NGFW)** em configuração de **Alta Disponibilidade (HA)**, acompanhados de licenciamento, instalação, treinamento e suporte técnico especializado.

3.3. A quantidade estimada está tecnicamente fundamentada no **Estudo Técnico Preliminar (SEI nº 0132562)**, onde se destaca a necessidade de funcionamento ininterrupto da solução de segurança perimetral, garantindo resiliência contra falhas e ataques, conforme as boas práticas de segurança da informação e os princípios de continuidade operacional. O ambiente em HA visa assegurar a operação estável de todos os serviços digitais do CFQ.

3.4. A solução proposta também contempla integração com diversos componentes da infraestrutura de TIC já existentes ou previstos, como switches, pontos de acesso Wi-Fi e sistemas de autenticação, evidenciando sua interdependência com outras contratações e viabilizando **economia de escala**, por meio da centralização da segurança, padronização de gestão e otimização do suporte técnico.

3.5. Em conformidade com o disposto no art. 11, incisos V e VI, da Instrução Normativa SEGES/ME nº 94/2022, apresentam-se a seguir as justificativas relativas à estimativa do **valor da contratação**, acompanhadas das respectivas memórias de cálculo e documentos de suporte.

3.6. **Estimativa do Valor da Contratação:** A **memória de cálculo do valor estimado** baseia-se no **Relatório de Pesquisa de Preços (SEI nº 0137811)**, que apresenta levantamento feito junto a **três fornecedores do setor privado** e ao **Painel de Preços do Governo Federal**, com base em contratações semelhantes já realizadas por órgãos da Administração Pública.

3.7. A análise dos dados seguiu os critérios da IN SEGES/ME nº 65/2021, com exclusão de valores inexequíveis ou excessivamente elevados. O resultado apontou como mais vantajosa a solução constante na **Ata de Registro de Preços nº 90020/2024 – IFSUL**, cujo valor total foi de **R$ 221.800,00**, incluindo:

- 2 appliances NGFW com licenciamento (R$ 155.200,00);
- 180 meses-hora de suporte técnico por 36 meses (R$ 66.600,00).

3.8. Os preços unitários referenciais constam no Termo de Referência (SEI nº 0205071) e na respectiva planilha detalhada da ARP. A adesão à Ata foi tecnicamente aprovada por apresentar compatibilidade com os requisitos funcionais e operacionais do CFQ, além de representar expressiva economia em relação às demais ofertas do mercado.

3.9.

4. ANÁLISE DE SOLUÇÕES

4.1. IDENTIFICAÇÃO DAS SOLUÇÕES

4.1.1. Após pesquisa de mercado, concluiu-se as soluções que se seguem:

4.1.1.1. **Solução 1 –** Firewall Appliance (Hardware dedicado)

a) Esta é a solução atualmente em utilização no CFQ.

b) Soluções de firewall baseadas em hardware dedicado, são projetadas para oferecer alto desempenho e funcionalidades avançadas de segurança. Esses dispositivos geralmente vêm com recursos integrados, como IDS/IPS, VPN, inspeção SSL/TLS, entre outros.

c) Um firewall appliance é uma solução de segurança que combina hardware dedicado e

software otimizado para fornecer proteção avançada à rede corporativa. Esses dispositivos são projetados especificamente para desempenhar funções de firewall de maneira eficiente, suportando funcionalidades de inspeção de tráfego, controle de aplicativos, VPN, prevenção contra intrusões (IPS) e detecção de ameaças avançadas. Os appliances são instalados fisicamente no local (on-premises) e atuam como o principal ponto de controle entre a rede interna da organização e a internet ou outras redes externas.

d) A solução 1 – Firewall Appliance, se configura como uma escolha viável, mantendo a estrutura e topologia já existentes no CFQ, uma vez que se busca uma proteção completa e ampla dos serviços de rede, considerando o aumento das demandas relacionadas a conexões e serviços a serem disponibilizados através da internet. A solução se sustenta na estabilidade da infraestrutura já estabelecida, oferece desempenho robusto e flexibilidade para personalizações necessárias. Além disso, facilita a integração com sistemas existentes, permite maior controle sobre a segurança e resulta em um investimento mais racional e gerenciável, alinhado ao crescimento contínuo das demandas de conectividade. Esses fatores, combinados, tornam essa solução a alternativa mais adequada para atender aos requisitos técnicos e operacionais do Conselho Federal de Química.

4.1.1.2. **Solução 2 –** Firewall na Nuvem (FaaS - Firewall as a Service)

a) Esta é uma solução baseada em nuvem que fornece segurança de rede como um serviço, eliminando a necessidade de hardware físico ou software dedicado no local. Essa abordagem centraliza as políticas de segurança, fornecendo proteção integrada para usuários, dispositivos e aplicações, independentemente de onde estejam localizados.

b) O FWaaS combina funcionalidades avançadas de firewall com flexibilidade e escalabilidade, ideal para organizações que possuem filiais distribuídas, que estão migrando para ambientes baseados em nuvem, multi-nuvem ou com equipes distribuídas, garantindo proteção uniforme e escalável sem a complexidade da gestão de infraestrutura física.

c) A solução 2 – Firewall na Nuvem (FaaS - Firewall as a Service) não se mostra uma solução viável tecnicamente pois, além de ser voltada para ambientes distribuídos e clusterizados, a infraestrutura é gerenciada pelo provedor, o que pode limitar personalizações específicas ou ajustes finos que seriam possíveis com soluções locais, além da dependência de uma conexão estável e de alta qualidade com a nuvem para evitar atrasos ou interrupções no tráfego inspecionado, nenhuma rota do tráfego de dados pode ter falhas ou todos os serviços podem ser comprometidos e, o modelo baseado em assinatura pode se tornar caro em médio e longo prazo, que é o caso desta contratação.

4.1.1.3. **Solução 3 –** Firewall Gerenciado (MSSP - Managed Security Service Provider)

a) O Firewall Gerenciado é uma solução oferecida por provedores de serviços de segurança gerenciada (MSSP - Managed Security Service Providers), que inclui o fornecimento, configuração, monitoramento e suporte contínuo de um firewall, de forma totalmente terceirizada.

b) Nesta métrica é criado um catálogo de serviço com os respectivos NMS [2] , bem como indicadores de desempenho e qualidade, definidos em contrato, que deverão ser observados.

c) Nesse modelo, o cliente delega a operação e a administração do firewall a um fornecedor especializado, que gerencia a infraestrutura e implementa políticas de segurança alinhadas às necessidades da organização. O serviço é geralmente contratado por meio de um modelo baseado em assinatura, com SLAs definidos para garantir níveis de desempenho, disponibilidade e suporte.

d) Este modelo apresenta a desvantagem de a gestão da infraestrutura e das políticas de firewall fica a cargo do MSSP, o que pode limitar a autonomia do cliente, a qualidade do serviço está diretamente ligada à capacidade técnica e ao SLA do MSSP e, o modelo de

assinatura pode ser custoso em longo prazo.

e) A Solução 3 é uma alternativa tecnicamente inviável para o CFQ devido à perda de autonomia no gerenciamento, à dependência de um provedor externo para o cumprimento dos SLAs, à potencial elevação dos custos ao longo do tempo e à dificuldade de integração plena com a infraestrutura interna da instituição. Essas limitações podem comprometer a robustez, a agilidade e a eficácia necessárias à proteção do ambiente digital, justificando a exclusão dessa solução no contexto atual.

4.1.1.4. **Solução 4 – Adesão à Ata de Registro de Preços (ARP nº 90020/2024 – IFSUL – UASG 158126)**

a) Como alternativa à contratação de serviços gerenciados de segurança (MSSP – Managed Security Service Provider), propõe-se a **adesão à Ata de Registro de Preços nº 90020/2024**, gerenciada pelo **Instituto Federal Sul-rio-grandense (IFSUL), UASG 158126**. A referida Ata contempla solução de segurança compatível com os requisitos técnicos levantados, incluindo funcionalidades equivalentes às previstas para firewall de próxima geração (Next-Generation Firewall – NGFW), além de recursos complementares de proteção de perímetro e controle de tráfego.

b) A adesão, prevista no art. 31 do Decreto nº 11.462/2023, representa uma solução **juridicamente válida, tecnicamente adequada e economicamente vantajosa**, considerando a compatibilidade entre os itens registrados e as necessidades deste órgão, bem como a economia de escala proporcionada por contratações centralizadas.

c) A escolha por essa solução visa atender aos princípios da eficiência e da economicidade, com significativa redução de esforço administrativo e redução do tempo necessário para implementação da solução. O fornecedor registrado foi consultado previamente e manifestou concordância quanto ao fornecimento, observando os quantitativos, prazos e condições estabelecidas.

d) A adoção desta solução está condicionada à anuência formal do órgão gerenciador, bem como à instrução processual com os documentos comprobatórios exigidos, incluindo análise de conformidade técnica, manifestação jurídica, proposta atualizada do fornecedor e demais elementos previstos na legislação aplicável.

4.2. ANÁLISE COMPARATIVA DE SOLUÇÕES:

4.2.1. No quadro abaixo, são apresentadas as características das soluções identificadas.

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3		X	
	Solução 4	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X

Requisito	Solução	Sim	Não	Não se aplica
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X

5. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

5.1. Do ponto de vista técnico, as soluções 2 e 3 são consideradas inviáveis conforme explicação nos itens 4.1.1.2 e 4.1.1.3.

6. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

6.1. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE E MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

6.1.1. Das soluções levantadas, será realizada análise de custo para a **Solução 1** – Firewall Appliance (Hardware dedicado) e **Solução 4**.

6.1.2. Segue abaixo os dados das pesquisas diretas com fornecedores e de preços públicos realizadas no painel de compras do Governo Federal com os preços obtidos conforme similaridade de escopo:

Solução 1 – Firewall Appliance (Hardware dedicado)		
Fonte	**Descrição**	**Valor total**
Garage Tech (CNPJ: 04.699.854/0001-69)	Appliance Firewall NGFW: instalação, configuração, suporte técnico, transferência de conhecimento e garantia.	R$ 344.597,90
Infoprotect (CNPJ: 35.489.078/0001-04)	Appliance Firewall NGFW: instalação, configuração, suporte técnico, transferência de conhecimento e garantia.	R$ 360.600,00
Estratégia IT (CNPJ: 15.813.403/0001-27)	Appliance Firewall NGFW: instalação, configuração, suporte técnico, transferência de conhecimento e garantia.	R$ 529.360,00
Altas Networks (CNPJ: 05.407.609/0002-84) Pregão 40/2023 - UASG 38908	Appliance Firewall NGFW: instalação, configuração, suporte técnico, transferência de conhecimento e garantia.	R$ 500.829,00
Digital Work (CNPJ: 03.688.545/0008-05) Pregão 30/2023 UASG 925124	Appliance Firewall NGFW: instalação, configuração, suporte técnico, transferência de conhecimento e garantia.	R$ 545.400,00
Approach Tecnologia (CNPJ: 24.376.542/0001-21) Pregão 90003/2024 UASG 154050	Appliance Firewall NGFW: instalação, configuração, suporte técnico, transferência de conhecimento e garantia.	R$ 480.000,00
Média do valor total estimado		**R$ 460.131,15**

Solução 4 – Adesão à Ata de Registro de Preços (ARP nº 90020/2024)		
Fonte	**Descrição**	**Valor total**
Sigma Tecnologia (CNPJ: 11.064.603/0002-54) SRP 90020/2024 - IFSUL - UASG 158126	Appliance Firewall NGFW: instalação, configuração, suporte técnico, transferência de conhecimento e garantia.	R$ 221.800,00
Valor total estimado		**R$ 221.800,00**

6.2. A adesão à Ata de Registro de Preços nº 90020/2024 (IFSUL – UASG 158126) apresenta a solução mais vantajosa para a Administração, com valor total de R$ 221.800,00, significativamente inferior à média do valor total estimado de R$ 460.131,15. A contratação por meio da referida Ata garante a economicidade, mantendo a conformidade técnica com os requisitos estabelecidos, além de assegurar

agilidade na implementação da solução, conforme detalhado no Relatório de Pesquisa de Preços (0137811).

7. JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO

7.1. Com a contratação da aplicação de firewall, busca-se a eficiência e facilidade de gerenciamento, uniformização do processo de trabalho, padronização de serviços e medição dos resultados através de níveis mínimos de serviços aceitáveis, aprimoramento e eficiência dos serviços de TIC, conforme a IN 94/2022.

7.2. A contratação pleiteada pretende garantir a continuidade do serviço de monitoramento e automatização da solução de segurança, visando assegurar a segurança da informação e o não vazamento de dados, observando os atuais normativos de segurança da informação, política de segurança da informação e CISv8, considerando que o advento de novas ameaças tecnológicas requer a adoção de novas soluções de segurança para garantir a integridade dos dados armazenados dentro da infraestrutura de TIC do Conselho Federal de Química.

7.3. A utilização de solução de segurança em appliance, aliado a uma detecção de ameaças, a análise e inspeção de tráfego Web, o gerenciamento inteligente de logs e relatórios, entre outras funcionalidades essenciais para a utilização segura da rede, sendo possível configurar regras de uso, realizar auditorias sobre acessos e o gerenciamento da utilização da Internet por usuários internos e visitantes, permitindo o uso consciente da rede de dados do CFQ.

7.4. Garantir a confiabilidade e segurança da informação que transitará pela rede do CFQ, assim como sua integridade, confidencialidade, autenticidade e disponibilidade de acesso, de forma a garantir a preservação e segurança da informação que, hoje, é considerada um dos ativos mais valiosos, não só pela sua importância estratégica, mas também por ser um elemento de fundamental importância para tomada de decisões pelas instituições e órgãos públicos.

7.5. Frente ao crescente avanço tecnológico das ameaças à segurança da informação, inclusive com utilização de IA (Inteligência Artificial) para comprometer sistemas e dados, torna-se necessário também evoluirmos no emprego de recursos profissionais atualizados com as mais recentes tecnologias para mitigar os potenciais ameaças aos dados deste Conselho Federal de Química.

7.6. Em setembro de 2020 a Lei Geral de Proteção de Dados (LGPD) nº 13.709, de 14 de agosto de 2018, entrou em vigência, ampliando as exigências do Marco Civil da Internet e reforçando a utilização de melhores práticas de mercado no que tange aspectos da Segurança da Informação. Tal Lei tem a prerrogativa de aplicar sanções administrativas pesadas para entidades privadas e públicas de até R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

7.7. A exemplificar, no caso de vazamento de informações de algum banco de dados de usuários desta Instituição, caracterizaria infração e aplicação de sanções. Diante disso, é imperioso que o CFQ se empenhe ao máximo, utilizando dos recursos tecnológicos de segurança disponíveis no mercado, em proteger as informações de seus profissionais do conselho, seus colaboradores, e afins, e toda informação inerente a existência e desempenho de suas finalidades e sob sua responsabilidade.

7.8. Neste momento nossa plataforma de segurança deve ser atualizada em razão do fim de vida da solução, informada pelo fabricante, tornando-se necessário o investimento em segurança da informação. Visto a elevada quantidade de ameaças existentes, que devem ser bloqueadas e que tais ameaças podem afetar os sistemas internos do conselho. Diante disso é imperioso a contratação de uma nova solução robusta.

7.9. Nesse contexto, a plataforma de appliance deverá ser voltada para missão crítica e 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.

7.10. A partir da necessidade de um modelo de serviço especializado, e com base no levantamento de mercado, a solução escolhida é aquela que mais se aproxima dos requisitos definidos pelo órgão, levando-se em conta os aspectos de economicidade, eficácia, eficiência e padronização.

7.11. Sendo assim, a solução escolhida é a que constitui na contratação de serviços especializados de operação de infraestrutura e atendimento ao usuário de Tecnologia da Informação e

Comunicação, vez que o CFQ necessita de corpo técnico operacional capacitado para a execução de determinadas atividades, conforme especificações no item 3.12, em quantidade suficiente para atender às demandas do CFQ.

7.12. A escolha desta solução deve-se ao fato de sua maior vantajosidade para a administração, tanto do ponto de vista econômico quanto técnico.

7.13. A presente contratação verificou a existência de Ata de Registro de Preços 90020/2024 vigente, constante no Relatório de Pesquisa de Preços (0137811), oriunda de processo licitatório realizado por órgão ou entidade da Administração Pública, cuja adesão está em conformidade com os requisitos legais e regulamentares. A referida Ata contempla os itens e as especificações técnicas que atendem integralmente às necessidades do órgão, conforme levantamento de demanda previamente realizado. Dessa forma, a adesão à Ata representa uma solução eficiente e vantajosa, possibilitando a contratação de bens/serviços de forma mais célere, com economia de recursos e esforço administrativo, sem prejuízo da qualidade e da conformidade com o interesse público.

7.14. **Benefícios a serem alcançados com a contratação**

7.14.1. Além do necessário aprimoramento do atual modelo de operação e sustentação de infraestrutura e atendimento ao usuário de TIC, o CFQ também pretende atingir os seguintes resultados, dentre outros:

a) Melhorar os níveis de disponibilidade do ambiente de infraestrutura de TIC, reduzindo a ocorrência de falhas e incidentes, e suportando a adequada execução das atividades finalísticas da instituição;

b) Prover os recursos técnicos adequados e necessários ao atendimento das demandas dos usuários e dos serviços de TIC suportados pela infraestrutura de tecnologia da informação;

c) Prover os recursos técnicos adequados e necessários ao suporte dos ambientes e das soluções de software hospedados pela infraestrutura de tecnologia da informação, ampliando a entrega de valor através dos serviços de TIC prestados pelo CFQ;

d) Aprimorar a capacidade técnica de atendimento de demandas, tratamento de incidentes e aplicação de mudanças no ambiente de infraestrutura de TIC, de forma alinhada aos requisitos de segurança e aos níveis mínimos de serviços demandados pela instituição;

e) Prover serviços técnicos especializados para contribuir com a mudança de sede, de forma que o projeto da infraestrutura de cabeamento estruturado possa ser analisado caso haja a necessidade de alterações no projeto, que seja feito antes da implantação, evitando assim possíveis alterações nas instalações após o término da obra; e

f) Manter a qualidade e eficiência dos serviços de TIC prestados ao CFQ após a finalização da mudança de sede.

7.15. Em conformidade com o disposto no **inciso XIII do art. 11 da Instrução Normativa SEGES/ME nº 94/2022**, conclui-se que a contratação da solução de **Firewall Next-Generation (NGFW)** em **Alta Disponibilidade (HA)**, conforme descrita no Estudo Técnico Preliminar (SEI nº 0132562), no Relatório de Pesquisa de Preços (SEI nº 0137811) e no Termo de Referência (SEI nº 0144917), **é adequada, necessária e suficiente para o atendimento da demanda institucional do Conselho Federal de Química – CFQ**.

7.16. A solução atende integralmente aos seguintes requisitos:

- **Necessidade técnica identificada**: substituição da atual solução de firewall, com fim de vida útil programado para 31/05/2025, garantindo continuidade operacional, segurança da informação e conformidade com a LGPD e demais normativos de TIC;
- **Alinhamento estratégico**: a contratação está alinhada ao Plano Diretor de TIC (PDTIC 2025–2027) e aos objetivos estratégicos do CFQ, especialmente no tocante à transformação digital, segurança cibernética e modernização da infraestrutura;

- **Solução validada tecnicamente e economicamente**: a opção pela adesão à Ata de Registro de Preços nº 90020/2024 – IFSUL foi considerada tecnicamente viável e economicamente vantajosa, após análise comparativa com outras ofertas do mercado;
- **Atendimento integral à demanda**: a proposta contempla, de forma unificada, todos os elementos necessários à implementação da solução: hardware, licenças, instalação, capacitação técnica e suporte, assegurando a operação plena desde a implantação;
- **Minimização de riscos**: a aquisição em modelo HA e com suporte técnico ativo mitiga riscos operacionais e assegura a resiliência da infraestrutura de TIC institucional;
- **Razoabilidade e proporcionalidade**: a especificação da solução, o quantitativo estimado e o valor contratado demonstram adequação ao porte da instituição, evitando tanto a subcontratação quanto a superdimensionamento.

7.17. Dessa forma, considera-se que a contratação proposta **é plenamente adequada ao atendimento da necessidade institucional do CFQ**, representando a solução tecnicamente mais eficaz, economicamente mais vantajosa e estrategicamente mais alinhada aos objetivos da Administração.

8. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

8.1. Tendo em vista a **solução 1,** única viável para o atual cenário e, considerando as propostas comerciais recebidas, bem como consulta ao Banco de Preços, verifica-se que a Ata de Registro de Preços é a melhor opção e oferece os serviços necessários.

8.2. A solução será composta por:

GRUPO ÚNICO				
ITEM	**ESPECIFICAÇÃO**	**UNIDADE DE MEDIDA**	**CATMAT/ CATSER**	**QUANT.**
1	Appliance de Firewall NGFW em Alta Disponibilidade (HA)	unidade	609340	2
2	Licenciamento para os recursos dos Firewall NGFW	unidade	27502	2
3	Serviço de Implantação	horas	27090	30
4	Treinamento técnico	horas	27740	40
5	Serviço suporte técnico	horas	27090	100

8.3. A adjudicação dos itens será realizada por grupo, considerando a necessidade de garantir a padronização, a compatibilidade técnica e a eficiência operacional na aquisição dos bens/serviços.

8.4. A opção pela adjudicação por grupo visa:

8.4.1. **Compatibilidade e Integração**: Os itens agrupados possuem interdependência técnica e funcional, sendo fundamental que sejam fornecidos por um único fornecedor para evitar incompatibilidades que possam comprometer a qualidade e a eficiência da execução.

8.4.2. **Racionalização dos Custos e da Logística**: A aquisição conjunta dos itens reduz custos administrativos e de gestão contratual, otimizando a execução do contrato e garantindo maior eficiência na entrega.

8.4.3. **Facilidade na Gestão e Suporte Técnico**: Um único fornecedor responsável pelos itens do grupo possibilita um suporte técnico mais eficiente, reduzindo riscos de conflitos entre diferentes fornecedores e garantindo um melhor acompanhamento das obrigações contratuais.

8.4.4. **Aumento da Competitividade e Melhor Oferta Global**: A adjudicação por grupo fomenta a participação de empresas capacitadas a fornecer todos os itens em conjunto, possibilitando propostas mais vantajosas e alinhadas ao interesse da Administração Pública.

8.5. Dessa forma, a adjudicação por grupo é a alternativa mais adequada para assegurar a economicidade, a eficiência e a qualidade na aquisição pretendida.

9. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

9.1. Considerando as propostas comerciais recebidas, bem como consulta ao Banco de Preços

e conforme tabelas de valores no item 6 e detalhamento de valores constantes do anexo I, tem-se que a estimativa do valor total desta contratação para o grupo único é de **R$ 221.800,00 (Duzentos e vinte e um mil e oitocentos reais)**, para a contratação do serviço técnico da empresa especializada que fará a instalação e configuração do serviço e, a contratação do serviço de suporte técnico especializado durante a vigência contratual.

9.2. Na tabela abaixo estão descritos os custos da solução:

Grupo	Descrição do Bem ou Serviço	Valor Total
Único	FIREWALL DE BORDA TIPO 4 COM LICENCIAMENTO PARA 36 MESES (Hardware e Licenciamento) e BANCO DE HORAS – SUPORTE TÉCNICO (HORAS)	**R$ 221.800,00 (Duzentos e vinte e um mil e oitocentos reais)**

10. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

10.1. Considerando as informações descritas neste Estudo Técnico, entende-se que a presente contratação atende a todos os requisitos necessários e se configura técnica e economicamente viável, e faz-se necessária para ampliar a capacidade operacional da Gerência de TI que confere proteção e disponibilização de serviços ao Conselho Federal de Química.

10.2. De acordo com a análise técnica constante no **Estudo Técnico Preliminar (SEI nº 0132562)** e no **Termo de Referência (SEI nº 0144917)**, conclui-se que **não é viável o parcelamento da solução**, pelos seguintes motivos:

10.2.1. **Indivisibilidade Técnica e Funcional**: Os appliances devem operar em modo **cluster de alta disponibilidade**, formando um sistema único, redundante e integrado. A aquisição fracionada comprometeria a performance, a segurança e a funcionalidade da solução, além de tornar a implantação inviável tecnicamente.

10.2.2. **Interdependência entre componentes e serviços**: A aquisição do hardware, das licenças de software, da instalação, do suporte e do treinamento técnico estão **intrinsecamente conectadas**, não podendo ser dissociadas sem afetar o funcionamento do sistema como um todo.

10.2.3. **Compatibilidade de versões e garantias**: O fornecimento unitário e coordenado garante que ambos os appliances estejam sob as **mesmas versões de firmware, políticas de segurança e cobertura de suporte**, o que seria dificultado em caso de contratação fracionada.

10.2.4. **Economia e eficiência na contratação**: A contratação integrada por meio da **adesão à Ata de Registro de Preços nº 90020/2024 – IFSUL** permite ganhos de escala, economia de tempo e redução de custos administrativos e operacionais, além de assegurar a obtenção de preços vantajosos para o conjunto da solução.

10.2.5. **Risco de incompatibilidades e aumento de custos futuros**: Parcelar a contratação, adquirindo os componentes de forma separada (hardware, licenças, serviços), poderia acarretar **aumento de custos, prazos maiores de implantação e riscos de incompatibilidade entre módulos ou fornecedores distintos**, além de dificultar o suporte técnico integrado.

Diante do exposto, **a solução deve ser contratada de forma indivisível**, por se tratar de um **sistema integrado e interdependente**, cuja funcionalidade e efetividade dependem da aquisição e implementação conjunta de todos os seus elementos constitutivos.

10.3. Encaminhe-se ao Gerente de Tecnologia da Informação, nos termos do Art. 11, inciso V, §2º da Instrução Normativa SGD/ME nº 94/2022.

11. JUSTIFICATIVA PARA A DESIGNAÇÃO DA AUTORIDADE MÁXIMA DA ÁREA DE TIC COMO INTEGRANTE REQUISITANTE

11.1. Conforme o § 4º do artigo 10 da IN SGD/ME nº 94/2022, a indicação e a designação de dirigente da Área de TIC para integrar a Equipe de Planejamento da Contratação somente poderá ocorrer mediante justificativa fundamentada nos autos.

11.2. Desta forma, justifica-se a participação do Gerente de Tecnologia da Informação como integrante requisitante no processo de planejamento em razão da definição das necessidades de negócio

para contratação relacionada à melhoria da infraestrutura computacional do CFQ.

12. ASSINATURAS

12.1. Conforme o § 2º do Art. 11 da IN SGD/ME nº 94, de 2022, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelo Integrante Técnico e Requisitante e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE	INTEGRANTE ADMINISTRATIVO
Renato Araújo Santana **Analista de TI**	Henrique Selvero Menezes Cardoso **Gerente de TI**	Deborah Kadja da Silva Alenar **Analista Administrativa**

13. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

13.1. Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

GERENTE EXECUTIVO
Weverton Borges do Nascimento de Sousa **Gerente-Executivo**

[1] No contexto de Tecnologias da Informação e Comunicação (TIC), o termo "appliance" se refere a um dispositivo ou sistema que combina hardware e software, sendo projetado para realizar uma função específica de maneira eficiente. Ao contrário de um simples software ou hardware isolado, um appliance TIC é uma solução integrada, muitas vezes pré-configurada e otimizada para executar tarefas específicas, como segurança, armazenamento de dados, monitoramento de rede ou gerenciamento de sistemas.

[2] NMS significa Network Management System (Sistema de Gerenciamento de Rede). Em um contexto de Firewall Gerenciado, o NMS é uma ferramenta ou conjunto de ferramentas que ajuda no monitoramento e na gestão de redes, incluindo a administração do firewall. Ele é responsável por fornecer visibilidade em tempo real sobre o desempenho da rede, configurando alertas para eventos de segurança, monitorando tráfego e gerenciando a infraestrutura de rede de forma proativa. Em soluções de MSSP, o NMS permite que o fornecedor de serviços de segurança tenha controle sobre a rede do cliente, facilitando a identificação de falhas, a análise de incidentes e o cumprimento dos SLAs acordados.

Documento assinado eletronicamente por **Renato Araujo Santana**, **Analista de Tecnologia da Informação**, em 12/06/2025, às 14:36, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 15 de novembro de 2020 .

Documento assinado eletronicamente por **Henrique Selvero Menezes Cardoso**, **Gerente**, em 12/06/2025, às 15:50, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 15 de novembro de 2020.

Documento assinado eletronicamente por **Deborah Kadja da Silva Alencar**, **Analista**, em 12/06/2025, às 17:18, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 15 de novembro de 2020.

Documento assinado eletronicamente por **Weverton Borges do Nascimento de Sousa**, **Gerente**, em 17/06/2025, às 19:53, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 15 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.cfq.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0205184** e o código CRC **9EF8655C**.

SCS Quadra 09 Edifício Parque Cidade Corporatre, Torre B, 9º andar
@cidade_unidade@/, CEP
Telefone: (61) 2099-3300 - www.cfq.org.br