Conselho Federal de Química

Plenário
Presidência
Gerência Executiva
Gerência de Tecnologia da Informação e Comunicação

TERMO DE REFERÊNCIA

Processo nº 2800.00.04327.2024

1. DAS CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de empresa especializada para fornecer Appliance Firewall Next-Generation em ambiente de Alta Disponibilidade (HA), com licença de uso, fonte redundante, instalação, treinamento e suporte técnico, conforme Ata de Registro de Preços do Pregão Eletrônico nº 90020/2024, gerenciada pelo Instituto Federal Sul-rio-grandense – IFSUL (UASG 158126).

GRUPO ÚNICO						
ITEM	**ESPECIFICAÇÃO**	**UNIDADE DE MEDIDA**	**CATMAT/ CATSER**	**QUANT.**	**VALOR UNITÁRIO**	**Valor Total**
1	Appliance de Firewall NGFW em Alta Disponibilidade (HA) + Licenciamento para os recursos dos Firewall NGFW	unidade	609340	2	R$ 77.600,00	R$ 155.200,00
2	Banco de Horas - suporte técnico por 36 meses	meses	27090	180	R$ 370,00	R$ 66.600,00
TOTAL					**R$ 221.800,00**	

1.2. O objeto desta contratação não se enquadra como sendo bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.3. O serviço objeto desta contratação é caracterizado como comum, uma vez que suas especificações seguem padrões usuais definidos no mercado.

1.4. O prazo de vigência da contratação é de 1 (um) ano contado na forma da Ata de Registro de Preços do Pregão Eletrônico nº 90020/2024, gerenciada pelo Instituto Federal Sul-rio-grandense – IFSUL.

1.5. A Ata de Registro de Preços do Pregão Eletrônico nº 90020/2024 oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

1.6. Estabeleceu-se como data final para a conclusão da contratação o dia **30/08/2025**, considerando a complexidade do objeto, os prazos legais aplicáveis e a capacidade de execução das áreas envolvidas.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

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.

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.

2.1. 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.

2.2. A contratação de uma solução de firewall de última geração (NGFW) é essencial para proteger o ambiente digital do CFQ contra ameaças cibernéticas sofisticadas. Essa solução não só monitora e controla o tráfego de rede, como também oferece recursos avançados – entre eles, detecção de intrusões, prevenção de ataques e inspeção profunda de pacotes. Com a implementação da tecnologia em ambiente de alta disponibilidade (HA), garante-se a continuidade dos serviços e a conformidade com as normas de proteção de dados.

2.3. 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

2.4. 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.

2.5. O objeto da contratação está alinhado com a Estratégia de Governo Digital 2018 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2025-2027 do Conselho Federal de Química, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
ID	**Objetivos Estratégicos**	**Nome do documento e vigência**
OE12	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/2025: 60% 3° TRI/2025: 40%

3. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

3.1. A solução mais viável e que representa as necessidades e melhorias no processo do atualização e segurança da informação do CFQ é a **solução 4**, conforme especificado no Estudo Técnico Preliminar (0132562) – Firewall Appliance (Hardware dedicado), por ser a mais vantajosa para a administração e totalmente viável tecnicamente.

3.2. 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.

3.3. Diante do cenário atual de constantes ameaças cibernéticas e ataques cada vez mais sofisticados, a segurança da informação tornou-se um fator crítico para a continuidade e resiliência dos negócios. O crescimento da digitalização, o aumento no volume de tráfego de dados e a necessidade de garantir a integridade, disponibilidade e confidencialidade das informações exigem a adoção de soluções avançadas de proteção.

3.4. A contratação de um **Firewall de próxima geração (NGFW - Next-Generation Firewall)** visa fortalecer a segurança da rede corporativa, proporcionando **controle granular do tráfego, prevenção contra ameaças avançadas, inspeção profunda de pacotes, segmentação de rede, integração com SD-WAN e proteção contra ataques direcionados**, como **ransomware, phishing e invasões não autorizadas**.

3.5. Além disso, a solução NGFW possibilita a **inspeção de tráfego criptografado (SSL/TLS)**, garantindo que ameaças ocultas em conexões seguras sejam identificadas e mitigadas em tempo real. Com a implementação de **políticas de acesso baseadas em identidade e aplicações**, a organização terá maior controle sobre o uso da rede, reduzindo riscos operacionais e melhorando a eficiência dos recursos de TIC.

3.6. Outro ponto essencial é a **alta disponibilidade (HA - High Availability)**, que assegura a continuidade dos serviços mesmo diante de falhas ou ataques, mantendo a produtividade da empresa e a conformidade com normas e regulamentações de segurança. A integração com plataformas de **gerenciamento centralizado e análise de ameaças** permitirá uma resposta mais ágil a incidentes, otimizando a gestão de riscos.

3.7. Portanto, a aquisição de uma solução de firewall NGFW é uma **estratégia essencial para modernizar a infraestrutura de segurança, proteger ativos digitais e garantir um ambiente confiável para operações empresariais**, reduzindo vulnerabilidades e assegurando a continuidade dos serviços com alto desempenho e proteção robusta.

3.8. Portanto, tem-se que a presente contratação fortalecerá consideravelmente a capacidade e eficiência do CFQ em lidar com os novos e crescentes desafios diários da segurança cibernética, cumprindo seu papel efetivo e suas competências legais.

3.9. Em atendimento ao disposto no art. 6º, §1º, da Instrução Normativa SGD/ME nº 94/2022, a área técnica manifesta-se quanto ao enquadramento do objeto como solução única de TIC.

3.10. Após análise do escopo da contratação, conclui-se que **a solução pretendida — firewall do tipo Next-Generation (NGFW) em alta disponibilidade — não configura solução única**.

3.11. A justificativa baseia-se na ampla oferta de produtos e fornecedores disponíveis no mercado, como evidenciado na pesquisa de preços (SEI nº 0137811), onde foram obtidas propostas de diferentes empresas, todas com capacidade de atender aos requisitos definidos de forma objetiva e aderente às boas práticas de segurança.

3.12. Além disso, as especificações técnicas adotadas não restringem a participação de múltiplos concorrentes, nem vinculam a contratação a fabricante, tecnologia ou solução exclusiva. A adesão à Ata de Registro de Preços nº 90020/2024 – IFSUL reforça a viabilidade concorrencial e a economicidade da contratação.

3.13. Dessa forma, **não se verifica qualquer característica que configure a solução como única**, estando o objeto em conformidade com os princípios de isonomia, ampla competitividade e

vantajosidade previstos na legislação vigente.

4. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

4.1. O objeto do presente Termo consiste na contratação de empresa especializada para fornecimento de Appliance Firewall NGFW – Next-Generation Firewall, com licença de uso, instalação, configuração, treinamento, transferência de conhecimento e suporte técnico especializado durante a vigência do contrato. A solução inclui a realização de manutenções corretivas e atualizações da ferramenta, durante toda a vigência do contrato, utilizando a infraestrutura de TIC do CFQ para a instalação dos sistemas.

4.2. Considerando a existência de Ata de Registro de Preços vigente, devidamente publicada e em conformidade com os normativos aplicáveis, será adotada a forma de contratação por meio de **adesão** à referida Ata. A escolha se fundamenta na compatibilidade dos itens registrados com as necessidades deste órgão, observando-se critérios de economicidade, celeridade processual e eficiência administrativa.

4.3. A adesão está prevista no art. 31 do Decreto nº 11.462/2023 e encontra respaldo na viabilidade técnica e na vantajosidade econômica, conforme demonstrado no Estudo Técnico Preliminar (ETP) e na análise de conformidade da área requisitante. Ademais, o fornecedor registrado manifestou concordância com o atendimento da demanda deste órgão, nos quantitativos e prazos estabelecidos.

4.4. A contratação será viabilizada mediante **adesão à Ata de Registro de Preços** do Pregão Eletrônico nº 90020/2024, gerenciada pelo **Instituto Federal Sul-rio-grandense – IFSUL (UASG 158126)**, nos termos do art. 31 do Decreto nº 11.462/2023 e demais normativos aplicáveis. A adesão está fundamentada na compatibilidade entre os itens registrados e a necessidade administrativa deste órgão, considerando especificações técnicas, condições comerciais, prazos de entrega e quantitativos adequados.

4.5. A opção pela adesão visa assegurar a **vantajosidade da contratação**, tanto sob o aspecto da economicidade quanto da celeridade processual, eliminando a necessidade de deflagração de novo certame licitatório para atendimento da demanda. A análise técnica e a pesquisa de mercado demonstraram que os preços registrados estão compatíveis com os valores praticados no setor, caracterizando-se como solução eficiente e tempestiva.

4.6. O fornecedor detentor da Ata foi previamente consultado e manifestou anuência quanto ao atendimento das condições estabelecidas por este órgão. A anuência formal do órgão gerenciador também será providenciada via painel gerencial informatizado do Governo Federal, conforme previsto na legislação vigente.

4.7. Todos os documentos comprobatórios da viabilidade e regularidade da adesão serão devidamente juntados aos autos processuais, observando-se os princípios da legalidade, publicidade e transparência.

5. CLASSIFICAÇÃO DOS SERVIÇOS E REQUISITOS DA CONTRATAÇÃO

5.1. Trata-se de serviço comum de caráter continuado, sem fornecimento de mão de obra em regime de dedicação exclusiva, a ser contratado por meio de adesão à Ata de Registro de Preços do Pregão Eletrônico nº 90020/2024, gerenciada pelo Instituto Federal Sul-rio-grandense – IFSUL (UASG 158126), tendo em vista obter a melhor relação entre custo e benefícios para a administração pública .

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

5.3. Os requisitos de negócio, de capacitação, legais, de segurança e privacidade, da arquitetura tecnológica, de projeto e implementação encontram-se descritos no Estudo Técnico Preliminar (0205184), sendo os mesmos apresentados para fins de habilitação no Pregão Eletrônico nº 90020/2024 Sistema de Registro de Preços do Instituto Federal Sul-rio-grandense – IFSUL.

5.4. **Requisito de Funcionalidade**

5.5. O sistema deverá executar a função de gateway de rede e monitorar todo tráfego de entrada e saída. A equipe de TIC do CFQ poderá intervir, realizando as alterações

necessárias sempre que oportuno.

5.6. **Requisitos de Manutenção e Suporte**

5.6.1. A manutenção do serviço será fornecida via suporte técnico por parte da empresa contratada.

5.6.2. No caso da ocorrência de incidentes que comprometam o serviço prestado, a contratada deverá realizar os procedimentos necessários para recolocar o software em seu pleno estado de funcionamento e de uso juntamente com a equipe de TI do CFQ.

5.6.3. A contratada deverá manter Central de Atendimento (sítio na Internet, e-mail e telefone) disponível durante o horário comercial, compreendido das 8h às 18h, de segunda a sexta-feira, obrigatoriamente em Português Brasileiro, para consultas e aberturas de chamados técnicos, ao longo de toda a vigência do contrato.

5.6.4. Os atendimentos de assistência técnica devem ser providos pela contratada em dias úteis, no período de 8h às 18h.

5.6.5. O atendimento será, preferencialmente, remoto com a possibilidade de intervenção local quando necessário, sempre acompanhado pela equipe técnica da contratante.

5.6.6. O suporte técnico deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos do produto, módulos e configurações referentes a solução.

5.6.7. A Contratada deve disponibilizar Central de Atendimento para Apoio aos usuários (web, e-mail e/ou telefone), disponível em horas úteis, com atendimento no idioma Português-Brasil, pelo período do contrato.

5.6.8. O sistema de abertura de chamados da contratada deverá estar disponível 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, em português ou por meio de um tradutor.

5.6.9. A abertura de chamados pela contratante poderá ser efetuada por telefone, por correio eletrônico e por sistema de controle de chamados, com e-mail de resposta do chamado aberto apresentando o número do ticket aberto, para acompanhamento da contratante.

5.6.10. A contratada deve disponibilizar para a contratante o fornecimento de acesso irrestrito (24 horas x 7 dias da semana) à área de suporte do fabricante, especialmente ao endereço eletrônico (*web site*), a toda a documentação técnica pertinente (guias de instalação/configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).

5.6.11. A contratada deverá oferecer manutenção e suporte técnico conforme o nível de severidade de cada chamado e dentro dos tempos de resposta definidos abaixo:

a) Quando um chamado for aberto pela contratante, a contratante deverá atribuir ao chamado o nível de severidade de acordo com a avaliação do tipo do problema e do impacto/dano.

b) A tabela 1 apresenta exemplos de problemas e respectivos níveis de severidade.

Nível de Severidade	Descrição de suporte e operações	Exemplos
Severidade A (Alta)	Um ou mais serviços não estão acessíveis ou não podem ser usados. A produção, as operações ou as datas limite para implantação são gravemente afetadas, ou há um grave impacto sobre a produção ou as atividades da instituição. Vários usuários ou serviços são afetados.	· Problemas generalizados para utilização da ferramenta; · Gerenciamento centralizado da ferramenta inacessível ou fora do ar; · Erro crítico ao atualizar o sistema.
Severidade B (Média)	O serviço pode ser usado, mas com limitações. A situação tem impacto operacional moderado e é possível lidar com ela durante o horário comercial. Um único usuário, cliente ou serviço é afetado parcial ou totalmente.	· Lentidão excessiva no sistema ou na máquina virtual, causado pela solução; · Falha ao executar ou instalar uma atualização.

Nível de Severidade	Descrição de suporte e operações	Exemplos
Severidade C (Baixa)	A situação tem impacto operacional mínimo. O problema é importante, mas não tem impacto expressivo na produtividade e no serviço atual do cliente. Um único usuário experimenta interrupção parcial, mas existe uma solução alternativa aceitável.	· Falso-positivo ou Falso-negativo em excesso, não causando problemas no bom andamento das atividades internas; · Lentidão do sistema.

Tabela 1 - Tipos de problemas e níveis de severidade

5.6.12. Quanto ao tempo de resposta inicial do suporte técnico, deverá ser baseado nos níveis de severidade descritos acima e no tipo de assinatura contratada. A tabela 2 abaixo descreve as metas de tempo de resposta:

Nível de severidade	Nível de serviço
Severidade A (Alta)	Disponível: 24/7 Tempo máximo de resposta: 8 (oito) horas
Severidade B (Média)	Disponível: 24/7 Tempo máximo de resposta: 24 (vinte e quatro) horas
Severidade C (Baixa)	Disponível: 24/7 Tempo máximo de resposta: Definido no momento da ocorrência, mas não superior a 3 (três) dias corridos

Tabela 2 - Tempo de Resposta

5.6.13. Todo o chamado somente será caracterizado como "encerrado" mediante concordância da contratante.

5.6.14. Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, esta deverá ser programada e planejada com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da contratante.

5.7. **Requisitos Temporais**

5.7.1. A contratada deverá disponibilizar, formalmente, os canais para suporte, no prazo máximo de 5 (cinco) dias úteis, após a assinatura do contrato.

5.7.2. Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

5.7.3. A apresentação dos planos e cronogramas de instalação e implantação deverão ocorrer no prazo máximo de 05 (cinco) dias úteis, após a assinatura do contrato, podendo ser prorrogado por igual período, desde que justificado pela contratada e autorizado pela contratante.

5.7.4. A execução dos planos de instalação e implantação deverão ocorrer no prazo máximo de 20 (vinte) dias úteis após a assinatura do contrato, podendo ser prorrogado por igual período, desde que justificado pela contratada e autorizado pela contratante.

5.8. **Requisitos Sociais, Ambientais e Culturais**

5.8.1. Recomenda-se, de acordo com Guia Nacional de Contratações Sustentáveis, inserir critérios de sustentabilidade ambiental nas especificações técnicas para aquisição de ativos de TI, os quais deverão atender aos requisitos técnicos que propiciam maior eficiência energética, maior vida útil e menor custo de manutenção.

5.8.2. Os critérios de sustentabilidade deverão ser fundamentados no desenvolvimento econômico, social e na conservação do meio ambiente, além de serem baseados nas diretrizes de sustentabilidade como menor impacto sobre recursos naturais, preferência para materiais, tecnologias e matérias-primas de origem local e maior eficiência na utilização de recursos naturais como água e energia.

5.8.3. A área técnica consultou o referido Guia para verificar se os serviços a serem adquiridos integram ou não a lista de objetos regidos por disposições normativas de caráter ambiental. Todavia, não foram identificados critérios aplicáveis, visto que a presente contratação se resume à aquisição de consultoria para instalação e configurações de software e respectivo suporte técnico, os quais não estão relacionados à incidência de impactos ambientais.

5.8.4. Ainda assim, destaca-se que todos os softwares e atualizações deverão ser disponibilizadas ao CFQ de forma eletrônica e pela internet, a fim de evitar o impacto da produção de CD/DVD sobre recursos naturais (flora, fauna, solo, água, ar) e de suas respectivas embalagens, de transporte e da necessidade de desfazimento futuro.

5.8.5. Nessa mesma linha, toda a documentação de software e base de conhecimento deverá estar disponível em formato digital.

5.8.6. O suporte técnico deverá ser prestado preferencialmente de forma remota, pela internet, de forma a evitar impacto sobre recursos naturais decorrentes do transporte de pessoas para o ambiente do CFQ.

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

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

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

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

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

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

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

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

5.9.8. 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.

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

5.9.10. 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;

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

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

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

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

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

5.9.16. 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;

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

5.9.18. Possuir ao menos 4 interfaces 1Gbps SFP;

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

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

5.9.21. Possuir interface do tipo console ou similar.

5.9.22. Possuir fonte 100-240VAC redundante.

5.10. **Requisitos de Projeto e de Implementação**

5.10.1. 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.

5.10.2. 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.

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

5.10.4. 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.

5.10.5. 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.

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

5.10.6.1. 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.

5.10.6.2. 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.

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

5.10.8. 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.

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

5.10.10. 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.

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

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

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

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

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

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

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

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

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

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

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

5.10.22. 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.

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

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

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

5.10.26. 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.

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

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

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

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

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

5.10.32. A solução deverá suportar operações em multicast.

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

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

5.10.35. A solução deverá permitir o agrupamento de serviços.

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

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

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

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

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

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

5.10.42. 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.

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

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

5.10.45. 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.

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

5.10.47. 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.

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

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

5.10.50. 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.

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

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

5.10.53. 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.

5.10.54. 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.

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

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

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

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

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

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

5.10.61. 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;

5.10.62. 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;

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

5.10.64. A solução deverá possuir reconhecimento de padrões;

5.10.65. A solução deverá possuir análise de protocolos;

5.10.66. A solução deverá possuir detecção de anomalias;

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

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

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

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

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

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

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

5.10.74. A solução deverá possuir alertas via correio eletrônico;

5.10.75. 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;

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

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

5.10.78. A solução deverá armazenar os logs de sessões;

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

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

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

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

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

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

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

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

5.10.87. 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.

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

5.10.88. A contratada deverá :

5.10.89. 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.

5.10.90. Instalar o equipamento no ambiente físico, incluindo racks, cabos e fontes de alimentação.

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

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

5.11. **Funcionalidade de VPN**

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

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

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

5.11.4. A solução deverá possuir suporte a VPN SSL.

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

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

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

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

5.11.9. 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.

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

5.12. **Funcionalidade de Controle de Aplicações**

5.12.1. A solução deverá possuir categoria pré-definidas, como alguns exemplos de tipos de

aplicações, como P2P; Instant Messaging; Web; Transferência de arquivos; VoIP.

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

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

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

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

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

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

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

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

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

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

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

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

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

5.13. **Funcionalidade de Balanceamento de Carga**

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

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

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

5.13.4. A solução deverá permitir persistência de sessão.

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

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

5.13.7. 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.

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

5.14. **Funcionalidade de SD-WAN**

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

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

5.14.3. A solução SD-WAN deverá suportar micro-segmentação de tráfego onde seja possível

aplicar políticas de navegação entre segmentos de LAN.

5.14.4. 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.

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

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

5.14.7. 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.

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

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

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

5.14.11. 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.

5.14.12. 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.

5.15. **Garantia, Suporte e Licenciamento**

5.15.1. 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;

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

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

a) 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.

b) 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.

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

d) A solução deve contemplar atualizações e garantia total por todo o período de vigência da licença.

e) O prazo de garantia do serviço da solução ofertada deverá corresponder ao período de vigência do contrato contados a partir da data de sua ativação.

f) A garantia dos produtos deve, obrigatoriamente, prover o direito a novas versões de todos os *softwares* contratados, nas mesmas condições durante todo o período de vigência do contrato, e permitir o acesso aos *sites* oficiais do fabricante para o suporte.

g) Toda a manutenção evolutiva, preventiva e corretiva ficará a cargo da contratada;

h) A contratada deverá prestar suporte técnico e garantir a atualização de versões durante todo o período contratual.

i) A contratada deverá sanar todos os vícios e defeitos da solução.

5.16. **Requisitos de Segurança da Informação e Privacidade**

5.16.1. 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.

5.16.2. A Solução contratada deverá possuir recursos que possibilitem a definição de regras e configurações aderentes à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

5.16.3. Todos os dados, documentos, projetos, estudos e trabalhos armazenados pelo CFQ na nuvem devem estar devidamente protegidos pelos mecanismos de segurança afetos à propriedade intelectual.

5.16.4. 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 o provedor, sem qualquer ônus para o CFQ, ensejando a reparação por perdas e danos sofridos pelo CFQ, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas.

5.16.5. O fornecedor deverá cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do CFQ.

5.16.6. Cada funcionário a serviço da contratada deverá estar ciente de que a estrutura computacional do órgão não poderá ser utilizada para fins particulares, sendo que quaisquer ações que tramitem em sua rede poderão ser auditadas.

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

5.16.8. A contratada deverá apresentar, na reunião inicial, relação nominal dos profissionais envolvidos na execução do contrato que deverão ter acesso às informações do CFQ, se for o caso, 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 ao CFQ.

5.16.9. A contratada deverá cumprir a Política de Segurança da Informação - POSIN 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;

5.16.10. A contratada não poderá veicular publicidade acerca dos serviços contratados, sem prévia e formal autorização por parte da contratante;

5.16.11. É vedado à contratada o acesso aos dados da contratante, sem prévia e formal autorização por parte da contratante;

5.16.12. A contratada deve comunicar formal e imediatamente a contratante qualquer ponto de fragilidade percebido que exponha.

5.17. **Garantia da Contratação**

5.17.1. As regras acerca da garantia são as estabelecidas no Termo de Referência, conforme Ata de Registro de Preços do Pregão Eletrônico nº 90020/2024, gerenciada pelo Instituto Federal Sul-rio-grandense – IFSUL.

6. TRANSFERÊNCIA DE TECNOLOGIA

6.1. A contratada deverá realizar a transferência de tecnologia, por meio de treinamento e

fornecimento de documentação técnica, visando capacitar a equipe de TIC do CFQ para operação, manutenção e gestão do sistema/produto fornecido, garantindo a autonomia do cliente no uso da solução.

7. PAPÉIS E RESPONSABILIDADES

7.1. **São obrigações da contratante:**

7.1.1. As regras acerca das obrigações da contrante são as estabelecidas no Termo de Referência, conforme Ata de Registro de Preços do Pregão Eletrônico nº 90020/2024, gerenciada pelo Instituto Federal Sul-rio-grandense – IFSUL.

7.2. **São obrigações da contratada:**

7.2.1. As regras acerca das obrigações da contratada são as estabelecidas no Termo de Referência, conforme Ata de Registro de Preços do Pregão Eletrônico nº 90020/2024, gerenciada pelo Instituto Federal Sul-rio-grandense – IFSUL.

8. MODELO DE EXECUÇÃO CONTRATUAL

8.1. As regras acerca do modelo da execução contratual são as estabelecidas no Termo de Referência, conforme Ata de Registro de Preços do Pregão Eletrônico nº 90020/2024, gerenciada pelo Instituto Federal Sul-rio-grandense – IFSUL.

9. MODELO DE GESTÃO DO CONTRATO

9.0.1. As regras acerca do modelo de gestão do contrato são as estabelecidas no Termo de Referência, conforme Ata de Registro de Preços do Pregão Eletrônico nº 90020/2024, gerenciada pelo Instituto Federal Sul-rio-grandense – IFSUL.

10. DOS CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

10.1. As regras acerca da entrega e critérios de aceitação do objeto são as estabelecidas no Termo de Referência, conforme Ata de Registro de Preços do Pregão Eletrônico nº 90020/2024, gerenciada pelo Instituto Federal Sul-rio-grandense – IFSUL.

11. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

11.1. O objeto da licitação tem a natureza de serviço comum, sem fornecimento de mão de obra em regime de dedicação exclusiva, e de caráter continuado, pois existe a necessidade de pleno funcionamento da solução, visto a essencialidade dos serviços e atividades a serem executadas pelo contratante.

11.1.1. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto nº 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.

11.1.2. 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.

11.1.3. Conforme explicitado no Estudo Técnico Preliminar, a presente contratação deverá ser processada na modalidade de adesão à ata, com vistas a obter a melhor proposta para a Administração Pública, evidenciada a significativa economia de recursos de tal alternativa.

11.2. **Da apresentação da Ata de Registro de Preços**

11.2.1. A empresa deverá apresentar a Ata de Registro de Preços referente ao Pregão Eletrônico n° 90020/2024 Sistema de Registro de Preços do Instituto Federal Sul-rio-grandense – IFSUL, devidamente assinada pelos responsáveis.

11.3. **Da Aplicação da Margem de Preferência**

11.3.1. Não se aplica, uma vez que para a licitação em questão será adotado o modelo de adesão à ata.

11.4. **Exigências de habilitação**

11.4.1. A empresa deverá apresentar a mesma documentação de qualificação técnica utilizada para fins de habilitação no Pregão Eletrônico nº 90020/2024 Sistema de Registro de Preços do Instituto Federal

Sul-rio-grandense – IFSUL.

12. DAS SANÇÕES ADMINISTRATIVAS

12.1. As regras acerca das sanções administrativas são as estabelecidas no Termo de Referência, conforme Ata de Registro de Preços do Pregão Eletrônico nº 90020/2024, gerenciada pelo Instituto Federal Sul-rio-grandense – IFSUL.

13. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

13.1. O preço estimado para a presente contratação é de **R$ 221.800,00 (Duzentos e vinte e um mil e oitocentos reais)**, conforme valores constantes na tabela abaixo e registrados na Ata de Registro de Preços do Pregão Eletrônico n° 90020/2024 do Instituto Federal Sul-rio-grandense – IFSUL.

13.2. Destaca-se que, no valor supracitado, estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro, garantia e suporte técnico especializado pelo prazo de 36 (trinta e seis) meses e outros necessários ao cumprimento integral do objeto da contratação.

Grupo Único	Valor Total
Appliance de segurança em HA e demais componentes de hardware, instalação, licenciamento da solução de segurança, treinamento técnico e suporte técnico durante a vigência contratual.	**R$ 221.800,00**

14. ADEQUAÇÃO ORÇAMENTÁRIA

14.1. A despesa correrá por conta de dotação orçamentária própria, prevista no orçamento do CFQ para o exercício de 2025, na seguinte classificação:

a) Centro de custo: 03.02.01.002 - Atividade de Gestão - Gerência de Tecnologia da Informação.

b) Conta Contábil para o hardware: 6.2.2.1.2.44.90.52.004 - Equipamentos de Informática.art.

14.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação do orçamento respectivo e liberação dos créditos correspondentes, mediante apostilamento.

14.3. CRONOGRAMA FÍSICO FINANCEIRO

14.3.1. O pagamento será efetuado após o recebimento definitivo da solução e liberação dos canais de suporte, conforme a tabela abaixo:

Item	Descrição	Forma de Desembolso
1	Appliance de segurança em HA e demais componentes de hardware, Instalação, Licenciamento da solução de segurança e Suporte técnico durante a vigência contratual.	**Único,** para Appliance, licenciamento e serviço técnico de implementação e suporte técnico pelo prazo contratual.
2	Treinamento técnico	Após a realização do treinamento técnico, sob demanda, conforma quantidade de horas efetivamente treinadas.

15. ANEXOS

15.1. Anexo I - Termo de Compromisso (0153586);

15.2. Anexo II - Termo de Ciência (0153588).

Integrante Requisitante	Integrante Técnico	Integrante Administrativo
Henrique Selvero Menezes Cardoso **Gerente de TI**	Renato Araújo Santana **Analista de TI**	Deborah Kadja da Silva Alencar **Analista Administrativa**

Autoridade Máxima da Área de TIC
Henrique Selvero Menezes Cardoso **Gerente de TI**

Aprovo,

Autoridade Competente	Autoridade Competente
Weverton Sousa **Gerente-Executivo**	José de Ribamar Oliveira Filho **Presidente do CFQ**

Documento assinado eletronicamente por **Renato Araujo Santana**, **Analista de Tecnologia da Informação**, em 12/06/2025, às 14:05, 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 15:51, 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 17:17, 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.

Documento assinado eletronicamente por **José de Ribamar Oliveira Filho**, **Presidente**, em 18/06/2025, às 16:15, 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 **0205071** e o código CRC **87D7E384**.

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