Conselho Federal de Química

Plenário
Presidência
Gerência Executiva
Gerência de Tecnologia da Informação e Comunicação

ESTUDO TÉCNICO PRELIMINAR: TI

Processo nº 2800.00.00429.2024

Contratação de empresa especializada para prestação de serviço de consultoria em implantação, instalação e configuração de ferramenta de software de segurança cibernética – SIEM – para o gerenciamento centralizado de logs de eventos de redes e alertas em tempo real de incidentes e eventuais ataques cibernéticos nos ativos de rede.

Referência: Art. 11 da IN nº 94/2022.

Histórico de Revisões

Data	Versão	Descrição	Autor
04/03/2024	1.0	Finalização da primeira versão do documento	Renato Araújo Santana
12/03/2024	1.1	Ajustes do modelo	Renato Araújo Santana
05/04/2024	1.2	Finalização de ajustes de preços	Renato Araújo Santana
09/04/2024	1.3	Revisão final	Henrique SM Cardoso
06/06/2024	1.4	Inclusão justificativa conforme recomendação ASJUR	Renato Araújo Santana

1. INTRODUÇÃO

1.1. Este estudo técnico preliminar tem como objetivo identificar a necessidade e justificar a contratação de empresa especializada para consultoria e implementação da ferramenta de segurança, destacando a importância do monitoramento de logs e análise e detecção de vulnerabilidades na segurança da informação do Conselho Federal de Química.

2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

2.1. O Conselho Federal de Química – CFQ, criado pela Lei 2.800, de 18 de junho de 1956, é uma autarquia federal que tem por finalidade promover a atividade plena da Química, com vistas a contribuir para o desenvolvimento sustentável do país.

2.2. Para o desempenho de suas atribuições, o CFQ conta com a estrutura organizacional composta por presidência, conselheiros, gerências executivas, áreas técnicas e administrativas.

2.3. A Tecnologia da Informação e Comunicação – TIC é um recurso do qual as organizações públicas dependem fundamentalmente para cumprir a sua missão institucional.

2.4. A Gerência de Tecnologia da Informação - GETIC contribui para os seguintes objetivos estratégicos do CFQ: “Adotar um sistema integrado e inovador de informação capaz de interligar o sistema CFQ/CRQs e as partes interessadas” e “Promover a inovação de processos e serviços, por meio da melhoria contínua e das ferramentas de Inteligência Artificial”.

2.5. O CFQ, atualmente, provê os acessos aos diversos serviços de TIC, como VOIP, e-mail, navegação web, vídeo conferência, hospedagem do website cfq.org.br, conexão remota, além de disponibilizar infraestrutura de compartilhamento interno de arquivos, computadores do tipo desktops e

notebooks para usos diversos pelos usuários da rede e serviços de e-mail e edição de arquivos on-line.

2.6. Com o aumento gradativo do uso de tecnologias hospedadas em nuvem, torna-se evidente a importância da ampliação das ferramentas que possibilitem manter o tráfego das informações no ambiente de redes seguro e confiável, com foco na melhoria e, principalmente, na disponibilidade dos serviços prestados, visando o correto andamento das atividades laborais dos colaboradores do CFQ.

2.7. A variedade de ataques cibernéticos, cada vez mais sofisticados e frequentes, exige que a instituição tenha capacidade de reconhecer e responder aos eventos e incidentes de redes de forma ágil e proativa, o que evidencia a necessidade de integrar os logs de registros de eventos das ferramentas de segurança em um único local, permitindo acesso rápido e em tempo real a alertas de vulnerabilidades de segurança.

2.8. Conselheiros, colaboradores e a sociedade fazem uso de diversos serviços disponibilizados via Internet, demandando constantemente comunicação através da rede mundial de computadores para realização de suas atividades, a exemplo do acesso ao serviço de e-mail e telefonia IP, bem como a iminente utilização de serviços corporativos em nuvem, tais como Office 365 e a implantação do Sistema Eletrônico de Informações – SEI no CFQ, devendo ainda ser considerada a implementação do trabalho remoto, com a demanda de acesso aos serviços via VPN.

2.9. Devido à criticidade desses serviços, faz-se necessário que o CFQ possua ferramentas para que a equipe de segurança da informação seja capaz de prevenir e executar medidas proativas de proteção e mitigação de riscos. Na última década, a tecnologia SIEM evoluiu para tornar a detecção de ameaças e a resposta a incidentes mais inteligentes e rápidas com a ajuda da inteligência artificial. Ele propicia à equipe de TIC a visibilidade completa sobre a rede de uma organização, ajudando administradores, operadores de SIEM, a monitorar a atividade de rede em sua infraestrutura, de forma centralizada e proativa.

2.10. Nesse contexto, para o adequado desempenho de suas atividades diárias, o CFQ necessita de ferramentas de segurança da informação que sejam sustentáveis, seguras, e que atendam aos requisitos de continuidade, segurança, melhores práticas de tecnologia da informação e governança, desempenho, disponibilidade, escalabilidade, economicidade, eficiência e ganho de escala, para sustentar a missão e alcançar a visão do CFQ.

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
N1	Eixo 1 - Modernização da Infraestrutura do Sistema CFQ/CRQs OE 12: Promover a inovação de processos e serviços, por meio da melhoria contínua e das ferramentas de Inteligência Artificial.	-Plano-Plurianual-CFQ-2022-2024; -Planejamento Estratégico do Sistema CFQ/CRQ-2018; -Mapa Estratégico / 2018 – 2028; -Plano Diretor de Tecnologia da Informação do CFQ 2023/2024.

ALINHAMENTO AO PDTIC 2023-2024		
ID	Ação do PDTIC	Meta do PDTIC associada
A61	Contratar solução de cibersegurança, auditoria e prevenção de ameaças.	Indicador: Contratação Realizada /Contratação Planejada Metas: 1° TRI/2023: 40% 2° TRI/2023: 60%

Identificação das necessidades tecnológicas	
1	**A18 Contratar solução de cibersegurança, auditoria e prevenção de ameaças**

A contratação pleiteada pretende garantir a continuidade dos serviços prestados pelo CFQ, a segurança da informação, o não vazamento de dados e a proteção a ataques de forma a informar proativamente à equipe de TIC do CFQ os alertas em tempo real, visando o correto andamento das rotinas internas do Conselho e observando os atuais normativos de segurança da informação e a política de segurança da informação.

O Wazuh é uma ferramenta de software open source de segurança da informação e de grande utilização em diversas empresas e órgãos governamentais pela sua versatilidade, e oferece um sistema avançado de gerenciamento de informações e eventos de segurança para monitorar a segurança da rede em tempo real.

Com a utilização do Wazuh, a equipe de TIC do CFQ irá integrar em uma só solução todos os eventos relacionados à infraestrutura de redes, o que permitirá monitorar e gerenciar de forma mais abrangente e ágil as vulnerabilidades e oportunidades de melhorias para a segurança da informação no ambiente do CFQ.

2.12. O atual cenário mundial tem como contexto o constante aumento e evolução dos ataques cibernéticos que possuem aderência de inteligência artificial para burlar sistemas e enganar usuários. Tal realidade tem por consequência a criação de ambientes de redes cada vez mais complexos, dificultando seu gerenciamento.

2.13. Os ataques cibernéticos estão se tornando cada vez mais sofisticados e frequentes, exigindo que as organizações adotem medidas proativas para proteger suas informações e sistemas. Nesse contexto, as soluções de Gerenciamento de Informações e Eventos de Segurança (SIEM, do inglês Security Information and Event Management) desempenham um papel vital. Elas permitem a detecção, análise e resposta eficaz a incidentes de segurança em tempo real.

2.14. Os serviços SIEM monitoram constantemente os usuários da rede, analisando padrões, transações, comportamento irregular, focando na identificação de ações classificadas como “estranhas” ao contexto da rede, contribuindo para o gerenciamento inteligente da rede por parte dos administradores.

2.15. Com a presente aquisição, pretende-se alcançar os seguintes resultados:

a) Integração de logs de eventos de rede;

b) Monitoramento em tempo real;

c) Alertas de incidentes de rede automatizados;

d) Correção de falhas de configurações; e

e) Provimento de disponibilidade, integridade e confiabilidade dos serviços de TIC do CFQ, internos e externos.

2.16. Conforme a necessidade evidenciada no tópico anterior e considerando que a contratação tem como objetivo o gerenciamento centralizado dos ativos de rede, das ferramentas de segurança da informação e dos eventos de rede e, considerando as diversas opções de ferramentas disponíveis no mercado, é de suma importância que a contratação possa agregar todas as ferramentas de propriedade do CFQ, bem como fornecer de forma clara uma visão completa e precisa de todo o ambiente de rede e de conformidade da segurança da informação com os normativos de regulação.

2.17. O sistema deverá permitir a identificação de acessos indevidos, alterações de arquivos e diretórios não autorizados, instalação de programas não permitidos, informar sobre eventos de falha de *login*, exibir painel *dashboard* para visualizar os dados em tempo real, visualizar a segurança de rede, verificar e identificar comportamentos incomuns no acesso a rede e seus dispositivos.

2.18. A infraestrutura a ser monitorada pela ferramenta de software é estimada conforme a lista a abaixo, podendo ser acrescida ou diminuída conforme as necessidades do CFQ:

a) 130 User Hosts/Endpoint BitDefender;

b) 05 Servidores Windows;

c) 20 Servidores Virtuais Linux;

d) 05 Switches Aruba 2930F + Switch (JL256A);

e) 01 Firewall SOPHOS - Next Generation;

f) 03 Roteadores MikroTik Routers and Wireless;

g) 07 Access Points Aruba;

h) 01 Servidor NAS (Network Attached Server);

i) Nuvem AWS;

j) Nuvem Microsoft - Office 365; e

k) VPN Sophos Connect.

2.19. A solução escolhida para ser o centralizador e gerenciador de logs e alertas dos ativos de rede do CFQ, conforme mencionado no caput, é o software WAZUH – Plataforma de Segurança Open Source, que unifica proteção SIEM e XDR para endpoints e cargas de trabalho em nuvem.

2.20. Wazuh unifica funções historicamente separadas em uma única arquitetura de agente e plataforma. A proteção é fornecida para nuvens públicas, nuvens privadas e datacenters locais. Ele fornece aos analistas correlação e contexto em tempo real. As respostas ativas são granulares, abrangendo a correção no dispositivo para que os endpoints sejam mantidos limpos e operacionais. A solução Wazuh Security Information and Event Management (SIEM) fornece monitoramento, deteção e alertas de eventos e incidentes de segurança.

2.21. Está disponível gratuitamente e adota uma abordagem de segurança de código aberto, que garante transparência, flexibilidade, melhoria constante e suporte gratuito da comunidade. Como uma plataforma de código aberto, o Wazuh se beneficia do rápido desenvolvimento de capacidades, oferece documentação abrangente e promove um alto envolvimento do usuário.

2.22. Wazuh é uma plataforma de código aberto para detecção de ameaças e resposta a incidentes, conhecida por sua adaptabilidade e capacidades de integração. A equipe de desenvolvimento aprimora continuamente a plataforma, apoiada por rigorosos processos de testes e auditoria. Incentivamos as contribuições dos usuários, como módulos funcionais e melhorias de código, que passam por verificações completas de garantia de qualidade para se alinharem aos nossos altos padrões.

2.23. Os usuários se beneficiam da flexibilidade para modificar o código-fonte, adaptando o Wazuh às suas necessidades específicas de segurança. Além disso, a compatibilidade do Wazuh com APIs e soluções de terceiros como VirusTotal, TheHive e PagerDuty enriquece sua funcionalidade, permitindo que ele sirva tanto como fonte quanto como receptor de dados de segurança. Essa combinação de desenvolvimento colaborativo, personalização e opções robustas de integração posiciona o Wazuh como uma ferramenta versátil no cenário da segurança cibernética.

2.24. Por oportuno, não há no Conselho, atualmente, colaboradores com conhecimentos técnicos necessários e suficientes para viabilizar toda a instalação, configuração e parametrização necessária para o correto funcionamento do referido software, de maneira que possibilite ao corpo técnico da GETIC seu uso integral para os fins a que se destinam, quais sejam, a proficiência no monitoramento e tratamentos de eventos relacionados à rede de dados e informações do CFQ, proporcionando um ambiente de rede mais seguro.

2.25. Outrossim, com o cenário exposto acima, a execução de todo o processo de implantação do software Wazuh demandaria tempo de aprendizado e testes que poderiam inviabilizar seu advento e inutilizar a ferramenta e seus benefícios, com resultados abaixo do esperado para o sistema em questão, não atendendo as expectativas do setor.

2.26. Por este motivo, resta imprescindível a contratação de empresa especializada para a realização dos serviços de instalação, configuração, parametrização e disponibilização dos painéis de monitoramento, serviços estes que serão acompanhados por servidores do CFQ, os quais direcionarão os técnicos da contratada quanto ao objetivo a ser alcançado ao final da implantação. Ainda, para que a implantação e os serviços a serem desenvolvidos a partir do sistema Wazuh tenham continuidade e forneçam informações objetivas referentes à rede de comunicação do Conselho, os servidores da GETIC receberão treinamento sobre todos os detalhes técnicos que forem utilizados e configurados, bem como as possibilidades de alterações e modificações que possam ser feitas e continuamente melhoradas pelos técnicos do CFQ.

2.27. Desta forma, a administração pública se beneficia na tripla relação entre **custo-benefício-tempo**, possibilitando à GETIC um ambiente robusto e confiável para as crescentes necessidades e demandas do Conselho Federal de Química.

3. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

3.1. Requisitos de Negócio

3.1.1. O desempenho das atividades finalísticas do CFQ depende de recursos de TIC, como equipamentos de uso diário, softwares, servidores, internet, rede de comunicação, serviços e outros.

3.1.2. Diante disso, para o adequado desempenho de suas atividades diárias, o CFQ produz inúmeros documentos e necessita de ferramentas e equipamentos que viabilizem a alta produtividade. Tal necessidade tende a crescer para sustentar o desenvolvimento da missão e alcançar a visão do CFQ: "Ser reconhecido como referência no desenvolvimento da Química no Brasil".

3.1.3. Do ponto de vista do negócio do CFQ, a solução contribuirá com a eficiência, produtividade, confiabilidade e disponibilidade dos serviços de TIC providos pelo Conselho, a exemplo dos serviços de acesso ao e-mail institucional e demais ferramentas do Microsoft 365, Sistema Eletrônico de Informações, acesso remoto via VPN em razão do modelo de teletrabalho híbrido, estações de trabalho e notebooks de uso geral dos colaboradores e servidores, bem como o site do Conselho Federal de Química – importantes instrumentos de comunicação e transparência, impactando positivamente na produtividade das áreas de negócio do CFQ, proporcionando um ambiente seguro e confiável para tramitação de documentos e procedimentos administrativos diários.

3.2. Requisitos Legais

3.2.1. 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);

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;

e) A prestação de serviços ao CFQ deverá estar alinhada à legislação brasileira no que se refere ao tratamento dos dados deste Conselho.

3.3. Requisitos de gerenciamento, monitoramento e suporte técnico

3.3.1. O sistema deverá monitorar a infraestrutura do CFQ no modelo 24x7, podendo a equipe de TI do CFQ intervir e fazer as devidas correções, quando necessário e oportuno.

3.3.2. 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.

3.3.3. 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.

3.3.4. Os atendimentos de consultoria e assistência técnica devem ser providos pela CONTRATADA em dias úteis, no período de 8h as 18h.

3.3.5. 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.

3.4. **Requisitos de Segurança**

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

3.4.2. 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.

3.4.3. 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.

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

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

3.4.6. 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.

3.4.7. 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.

3.4.8. 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.

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

3.5.1. A proponente deverá informar em sua especificação técnica as configurações necessárias de hardware, para que a solução de monitoramento funcione de forma adequada. Também deverá implantar o sistema na versão estável mais atual disponível, e deverá ser implantada também as versões mais atuais dos *plugins* e sistemas adicionais que forem necessários serem instalados em conjunto.

3.5.2. Durante a implantação a CONTRATADA deverá auxiliar a equipe técnica do Conselho Federal de Química nas configurações para conexão dos equipamentos ao sistema de monitoramento.

3.5.3. A proponente deverá criar *triggers*, *plugins* e *templates* personalizados para obtenção das informações dos dispositivos a serem monitorados e para adição de novos objetos.

3.5.4. Para instalação da solução a CONTRATANTE fornecerá infraestrutura com hardware de, no mínimo:

3.5.4.1. 100GB de armazenamento;

3.5.4.2. CPU 8 cores;

3.5.4.3. 16GB de memória RAM.

3.6. **Requisitos de Projeto e de Implementação**

3.6.1. A consultoria para implementação da solução de monitoramento consiste na ação de executar todo o escopo de planejamento, instalação e configurações da solução de software adquirida.

3.6.2. A CONTRATADA deverá analisar a estrutura atual e planejar as configurações de acordo com o ambiente produtivo do CFQ.

3.6.3. Devem fazer parte do escopo de instalação e configuração da ferramenta contratada:

3.6.3.1. Informar os requisitos de hardware necessário para implantação do sistema de monitoramento de segurança;

3.6.3.2. Auxiliar na configuração dos elementos monitorados;

3.6.3.3. Implantar o software de monitoramento de segurança;

3.6.3.4. Customizar o sistema de monitoramento de segurança conforme necessidades do Conselho Federal de Química;

3.6.3.5. Implementar painel dashboard conforme necessidades do Conselho Federal de Química;

3.6.3.6. Implementar painel dashboard de incidentes com classificação dos incidentes de segurança conforme definição de criticidade, status etc.;

3.6.3.7. Implementar painel de vulnerabilidades;

3.6.3.8. Customizar os painéis dashboard conforme necessidades do Conselho Federal de Química;

3.6.3.9. Levantar as regras de negócio para monitoramento de segurança dos ativos;

3.6.3.10. Desenvolver relatórios customizados de acesso e login a rede;

3.6.3.11. Desenvolver scripts com os parâmetros de monitoração de segurança conforme necessidade do Conselho Federal de Química;

3.6.3.12. Implementar script para envio de alertas de falhas, anomalias e alterações, gráfico de dados e ao sistema de e-mails do Conselho Federal de Química;

3.6.3.13. Registrar e armazenar dados estatísticos para auxiliar no diagnóstico das possíveis causas de tentativas de invasão;

3.6.3.14. Elaborar cronograma detalhado para implantação do sistema, descrevendo as etapas para a implantação desde as atividades de planejamento até a implantação final.

3.7. **Requisitos de Formação da Equipe**

3.7.1. A equipe da CONTRATADA responsável pela análise e atendimento dos chamados criados por este Conselho deverá possuir conhecimento comprovado acerca da solução escolhida e comprovação dos serviços fornecidos e já prestados a fim de o CFQ aferir a veracidade das experiências informadas.

3.7.2. A equipe técnica da CONTRATADA deverá realizar treinamento para a equipe técnica da CONTRATANTE, abordando os conceitos, configurações e parâmetros da implementação do sistema de monitoramento.

3.7.3. O treinamento a que se refere o item 1.24.2 deverá ter, no mínimo, 8 horas de conteúdo teórico e prático e deverá constar de material de consulta com todos os conceitos a respeito da implementação, parâmetros e configurações do sistema.

3.7.4. O treinamento operacional deverá fornecer certificação de conclusão aos participantes.

3.8. **Requisitos de Metodologia de Trabalho**

3.8.1. Após a reunião inicial os serviços deverão ser iniciados em até 15 dias, podendo ser prorrogado por igual período, desde que justificado pela CONTRATADA e aceito pela CONTRATANTE.

3.9. **Requisitos de Limite Geográfico**

3.9.1. Em conformidade com o disposto na NC 14/IN01/DSIC/GSIPR, os dados e informações do CFQ devem residir exclusivamente em território nacional, incluindo replicação e cópias de segurança (*backups*), de modo que o CFQ disponha de todas as garantias da legislação brasileira, enquanto tomadora do serviço e responsável pela guarda das informações armazenadas em nuvem.

4. ANÁLISE DE SOLUÇÕES

4.1. IDENTIFICAÇÃO DAS SOLUÇÕES:

4.1.1. Foi realizado um levantamento de soluções disponíveis, considerando as alternativas de mercado e, que podem atender à necessidade do CFQ, bem como as necessidades de adequação de ambiente e disponibilização de infraestrutura para instalação da solução escolhida, na sede do Conselho Federal de Química, que viabilize a execução contratual.

4.1.2. Verificaram-se como possíveis soluções a:

4.1.2.1. 1 - Aquisição de licenciamento de ferramenta de software comercial;

4.1.2.2. 2 - Implementação de ferramenta de software Open Source;

4.1.2.3. 3 - Implantação de SOC – Security Operation Center.

4.1.3. Abaixo está o detalhamento comparativo das soluções.

4.2. **A solução 1 –** Aquisição de licenciamento de ferramenta de software proprietária – corresponde à aquisição de licenciamento de uso de ferramenta de software proprietária para gerenciamento e armazenamento dos logs dos ativos de rede do CFQ, e não inclui os serviços de instalação, configuração e treinamento da equipe da Gerência de TI para as funcionalidades da ferramenta.

4.3. A **solução 2** - Implementação de ferramenta de software Open Source – consiste na instalação e configuração do monitoramento dos ativos de rede do CFQ com a utilização de ferramenta de software de código aberto, amplamente utilizada no mercado de segurança da informação.

4.4. A **solução 3** - Implantação de SOC – Security Operation Center – visa a criação de um centro de operações de segurança completo, com monitoramento 24x7, geração de relatórios, análises de alertas, resposta a incidentes, priorização de alterações, avaliações periódicas de segurança, gestão das vulnerabilidades do ambiente e outros serviços que complementem a operação de segurança, tornando o ambiente de rede completamente monitorado e gerenciado conforme as melhores práticas de mercado e os normativos regulamentares.

4.5. ANÁLISE COMPARATIVA DE SOLUÇÕES:

4.5.1. 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		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3			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
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 1			X

Requisito	Solução	Sim	Não	Não se aplica
A Solução é aderente às orientações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 2			X
	Solução 3			X
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

4.6. Do ponto de vista técnico, todas as soluções tecnológicas avaliadas são consideradas viáveis. Sendo assim, será demostrado a seguir a comparação entre os custos associados à cada solução.

5. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

5.1. Não se aplica.

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. A comparação de custos das soluções 1, 2 e 3 foi realizada por meio de pesquisa direta com fornecedores e, com as empresas proprietárias dos direitos de uso para as ferramentas da solução 1. Os valores obtidos são resumidos nas tabelas abaixo.

Solução 1 – Aquisição de licenciamento de ferramenta de software proprietária		
Fonte	**Descrição**	**Valor total**
Empresa BLUE TRUST/IBM	Subscrição (assinatura) - IBM Security QRadar SIEM	R$ 77.544,88 (para 12 meses)
	Implantação	R$ 11.500,00
	Treinamento (16 horas)	R$ 8.700,00
	TOTAL	**R$ 97.744,88**

Solução 2 – Implementação de ferramenta de software Open Source		
Fonte	**Descrição**	**Valor total**
Empresa LINUX SOLUTIONS	Software WAZUH - Suporte técnico especializado - instalação, configuração, treinamento	R$ 9.990,00
	Consultoria - Suporte técnico - 120 horas/ano	R$ 1.270,00 (R$15.240,00 para 12 meses)
	TOTAL	**R$ 25.230,00**
Empresa DIAZERO	Software WAZUH - Suporte técnico especializado - instalação, configuração, treinamento + Consultoria/Suporte técnico anual	R$ 74.980,00
	TOTAL	**R$ 74.980,00**
Empresa 4LINUX	Software Graylog + Grafana - Suporte técnico especializado - instalação, configuração, treinamento	R$ 72.246,68
	TOTAL	**R$ 72.246,68**

Solução 3 – Implementação de SOC		
Fonte	**Descrição**	**Valor total**
Empresa DIAZERO	Software WAZUH - Suporte técnico especializado - instalação, configuração, overview + equipe resposta incidentes, relatórios - SOC N1	R$ 17.895,00 (R$ 214.740,00 para 12 meses)

	TOTAL	**R$ 214.740,00**
Empresa INFOPROTECT	Software WAZUH - Suporte técnico especializado - instalação, configuração, overview + equipe resposta incidentes, relatórios - SOC N1	R$ 19.000,00 (R$ 228.000,00 para 12 meses)
	TOTAL	**R$ 228.000,00**
Empresa BLUE TRUST/IBM	Subscrição (assinatura) - IBM Security QRadar SIEM	R$ 77.544,88 (para 12 meses)
	Implantação	R$ 11.500,00
	Treinamento (16 horas)	R$ 8.700,00
	Serviço Técnico Especializado – gerenciamento SOC N1	R$ 4.200,00/mês (R$ 50.400,00)
	TOTAL	**R$ 148.144,00 para 12 meses**

6.1.2. Também foram realizadas pesquisas de preços públicos no painel de compras do Governo Federal, e os preços obtidos conforme similaridade de escopo e aplicação estão detalhados a seguir.

Implementação de ferramenta de software Open Source		
Fonte	**Descrição**	**Valor total**
Empresa LANLINK	Suporte técnico especializado - instalação, configuração, parametrização e treinamento	R$ 33.220,43
	TOTAL	**R$ 33.220,43**
Empresa TIQUI SOLUTIONS	Suporte técnico especializado - instalação, configuração, parametrização e treinamento	R$ 36.000,00
	TOTAL	**R$ 36.000,00**

6.1.3. Conforme as tabelas acima, fica evidenciado uma grande variação dos preços entre as 3 soluções apresentadas. Todas as alternativas de solução são viáveis economicamente, sendo que os motivos técnicos e econômicos para a justificação da solução escolhida encontram-se no item que se segue.

6.1.4. Toda a documentação comprobatória dos preços coletados constam detalhadas no anexo I – Detalhamento de propostas.

7. JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO

7.1. Dentre as soluções pesquisadas, a escolhida foi a implementação de ferramenta de segurança Open Source WAZUH, com suporte técnico de empresa especializada e com know-how e reconhecimento no mercado de cibersegurança, para a realização de instalação, parametrização, configuração e criação de painéis de monitoramento, treinamento e repasse de conhecimento para a equipe de TI deste Conselho, adicionado à celebração de contrato de suporte anual com horas de consultoria técnica prestadas à equipe de TI do CFQ para eventuais ajustes e melhorias nas configurações e modelos de visualizações de alertas.

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

7.3. Tal solução atende a todos os requisitos de segurança da informação necessários à sua implantação, bem como apresenta as ferramentas necessárias para o atendimento com resultados satisfatórios às necessidades técnicas do CFQ em vistas a manter o controle da segurança da informação, dos ativos de rede e do pleno funcionamento do ambiente computacional.

7.4. Além do citado acima, tanto a equipe de TI quanto a própria instituição vêm adquirindo gradualmente uma maior maturidade nos processos de segurança cibernética, com recentes publicações e atualizações de normativos relativos à segurança cibernética dentro do ambiente do CFQ, e adoção de novas políticas e processos que contribuem para esta evolução de maturidade.

7.5. Dentre os principais benefícios desta aquisição, destacam-se, portanto, a economia de recursos, a manutenção da disponibilidade, confiabilidade, integridade e autenticidade dos serviços, a manutenção da segurança contra novas ameaças que surgem diariamente, além de contribuir para o crescimento gradativo e contínuo da maturidade de segurança e para que a equipe de TI do CFQ amplie

sua capacidade de monitorar e diagnosticar vulnerabilidades e eventuais falhas e gargalos no ambiente de redes interno, nos serviços afetos à sua responsabilidade.

7.6. Com a utilização do software WAZUH, de código aberto e licenciamento gratuito, e que oferece os recursos necessários à necessidade atual do CFQ, faz-se necessário a contratação de empresa parceira especializada para efetuar a implantação, desde o fornecimento das características de hardware a ser utilizada à finalização da configuração de alertas e painéis, bem como o treinamento para que a equipe de TI possa efetivamente manusear, analisar e tratar as informações que serão extraídas do monitoramento.

7.7. Neste momento, em que o Conselho Federal de Química, através da Gerência de TI, vem aumentando seu nível de comprometimento com a segurança da informação, fortalecendo o uso das ferramentas disponíveis e ampliando a capacidade de monitorar e avaliar, não se faz oportuna a contratação por meio de outra solução, visto que envolveria uma alta curva de aprendizado e socialização com uma ferramenta proprietária gerando, além de redução dos níveis de produtividade, um aumento considerável dos investimentos em aquisição de licenciamentos e em treinamentos, o que prejudica e compromete a economicidade e eficiência da administração.

7.8. Bem como, a contratação de um Security Operation Center - SOC, acarretaria, além de um custo fixo mensal elevado já evidenciado nas tabelas acima, a necessidade de que a equipe de TI já possuísse pleno domínio de todas as ferramentas, técnicas de defesa e, principalmente, o conhecimento prático do monitoramento e resposta a incidentes para que pudesse orientar e gerir a equipe terceirizada de acordo com o ambiente do CFQ.

7.9. A necessidade de adaptação e obtenção do conhecimento através de uma ferramenta Open Source juntamente com uma consultoria especializada fará com que a equipe da Gerencia de TI do CFQ adquira e pratique suas habilidades para fornecer a este Conselho as melhores práticas de segurança existente no mercado, com a melhor relação entre custo e benefício para a administração.

7.10. Tendo como base a garantia dos preceitos fundamentais da segurança da informação e segurança cibernética, a manutenção da infraestrutura em pleno funcionamento, a evolução na aplicação de políticas e regras conforme os normativos mais recentes publicados pela Secretaria de Governo Digital – SGD/ME e do Gabinete de Segurança Institucional – GSI/PR, tal contratação é a mais vantajosa do ponto de vista econômico e também do ponto de vista técnico, aliada à facilidade de gestão e do conhecimento disponível à sua operação.

7.11. Portanto, tem-se que a presente contratação fortalecerá sobremaneira 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.

8. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

8.1. Tendo em vista que a solução 2 é a mais viável para o atual cenário e, considerando as propostas comerciais recebidas, possui um custo consideravelmente menor, verifica-se que esta é a melhor opção e oferece os serviços necessários.

8.2. A solução será composta por:

Quantidade	Solução
1	Software WAZUH - Serviços de Instalação, Transição e Configuração / Parametrização de Software;
	Suporte técnico especializado por 12 (doze) meses.

8.3. O servidor físico que hospedará a aplicação será instalado e fornecido pelo CFQ com as características de hardware fornecidas pela CONTRATADA.

9. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

9.1. Considerando as propostas comerciais recebidas, conforme tabelas de valores no item 6 e anexo I, tem-se que a estimativa do valor total desta contratação é de **R$ 36.000,00 (trinta e seis mil 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 pelo prazo de 12 meses.

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

Item	Descrição do Bem ou Serviço	Qtd.	Valor Total (12 meses)
1	Serviços de Instalação, Transição e Configuração / Parametrização de Software; e suporte técnico especializado por 12 meses	1	R$ 36.000,00

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. 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**	Daniela Vasconcelos de Oliveira **Analista Administrativo**

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.

RENATO DE MELO TEIXEIRA
Gerente-Executivo

JOSÉ DE RIBAMAR OLIVEIRA FILHO
Presidente

Documento assinado eletronicamente por **Renato Araujo Santana**, **Analista de Tecnologia da Informação**, em 06/06/2024, às 17:43, 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 07/06/2024, às 10:33, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 15 de novembro de 2020.

Documento assinado eletronicamente por **Daniela Vasconcelos de Oliveira**, **Integrante Administrativo da Equipe de Planejamento**, em 07/06/2024, às 10:45, conforme horário oficial de Brasília, com fundamento no Decreto nº 10.543, de 15 de novembro de 2020 .

Documento assinado eletronicamente por **Renato de Melo Teixeira**, **Gerente**, em 07/06/2024, às 15:29, 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 09/07/2024, às 14:32, 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 **0075155** e o código CRC **FE109AD5**.

Referência: Processo nº 2800.00.00429.2024 SEI nº 0075155

SCS Quadra 09, Edifício Parque Cidade Corporate, Torre B, 9º andar
Brasília/DF, CEP 70.308-200
Telefone: (61) 2099-3300 - www.cfq.org.br