CIASC
CENTRO DE INFORMÁTICA
E AUTOMAÇÃO DO ESTADO DE SANTA CATARINA S.A.

ANEXO II: ESTUDO TÉCNICO PRELIMINAR

I - INFORMAÇÕES GERAIS

1. Equipe de Planejamento

Nome	Cargo/função	E-mail
DIEGO LOPES DA CRUZ	Coordenador de Cibersegurança	diegolc@ciasc.sc.gov.br
ANDRE DAROS	Coordenador de Gestão de Redes	adaros@ciasc.sc.gov.br
BRUNNO NASCIMENTO LOPES	Gerente de Redes e Data Center	brunnonl@ciasc.sc.gov.br

2. Descrição do problema a ser resolvido ou da necessidade apresentada (art. 18, § 1º, I, da Lei Federal nº 14.133, de 2021).

O principal interesse público a ser atendido é a continuidade dos serviços de segurança de TI, garantindo a atualização tecnológica, e procurando evitar a interrupção da prestação dos serviços públicos do CIASC, o que causaria transtornos aos servidores e comunidade em geral que necessitam acessar os sistemas armazenados no Data Center de governo. Além disso, a infraestrutura de segurança que se deseja adquirir é responsável por garantir o acesso à Internet de forma segura para os clientes do CIASC, identificando e mitigando riscos como ataques à infraestrutura de TI do Governo, invasões a redes privadas, roubos de dados e outras ameaças cibernéticas.

Identificou-se as necessidades que serão apresentadas em partes:

- Em 2020, o CIASC fez uma licitação e adquiriu a solução de *next generation Firewalls* da marca FORTINET, pois havia a necessidade de aumentar a visibilidade de segurança de sua rede e Data Center, com novas funcionalidades que os Firewalls antigos tradicionais não haviam.
- Nessa solução, foram adquiridas dois clusters: um para para Provimento de Internet (FG-2200E) e outro par para Data Center (FG-3301E), e também a solução de gerenciamento centralizado (FortiManager) e gestão de logs (FortiAnalyzer), todos estes com licenciamento, suporte e garantia para 60 meses.
- Os firewalls do modelo FG-2200E (provimento) da FORTINET estão atingindo as suas capacidades máximas de operação, já que nossos links de internet aumentaram bastante nos últimos anos, e o licenciamento para atualização

das funcionalidades está por acabar. A situação possível é a troca do equipamento, por um modelo com maior capacidade, garantindo as atividades por um tempo muito maior.

- Os firewalls do modelo FG-3301E da FORTINET ainda esta com a capacidade de operação dentro dos limites toleráveis, mas o contrato de suporte e atualizações de 5 anos está por acabar em 21/07/2026 e também acreditamos que não consiga atender para os próximos 5 anos. Nesse caso, após análise da cotação enviada para renovação de licenças do FG-3301E, vimos que representa 70% do valor do equipamento e ainda existe de não ficar sobrecarregado nos próximos anos. Portanto, diante dessa analise, é recomendado trocar também o conjunto por um hardware maior ao invés de optar somente pela renovação de licenças.

Existe a necessidade de assegurar o funcionamento da solução de segurança de redes e ampliação de sua capacidade para provimento de internet. O processo do CIASC segue especificações semelhantes às utilizadas em anos anteriores, e tem por objetivo complementar e dar manutenção na segurança da comunicação do CIASC, tendo apresentado bom resultado (custo x benefício) e também aproveitar a integração com os demais produtos do fabricante Fortinet, como por exemplo VPN Forticlient, FortiManager e FortiAnalyzer.

3. Demonstração da previsão da contratação com o Plano Anual de Compras (art. 18, § 1º, II, da Lei Federal nº 14.133, de 2021).

A aquisição de equipamentos de FIREWALL para o CIASC consta no Calendário de Licitações/Plano Anual de Compras, descrita como “Ampliação de hardware ou renovação de licenças e suporte da plataforma de segurança Fortinet Fortigate (firewalls)” (Item 456), objetivando a atualização da infraestrutura de rede. A definição dos quantitativos e necessidades tem como base o histórico de eventos e crescimento das atividades. Dando continuidade à ampliação da rede e melhoria da rede lógica do CIASC, que foi elaborado pela GERED e que faz parte do planejamento estratégico atendendo as metas de comunicação.

4. Descrição dos requisitos da potencial contratação (art. 18, § 1º, III, da Lei Federal nº 14.133, de 2021)

Os firewalls de perímetro atuam como uma barreira essencial, filtrando o tráfego de rede e aplicando regras de bloqueio nas camadas de rede e transporte do modelo OSI. Eles fornecem funcionalidades como:

- **Filtro de Botnet:** Proteção contra redes de computadores infectados.
- **Gateway (Antivírus, Anti-Spyware, Prevenção de Intrusão):** Defesa contra softwares maliciosos e tentativas de invasão.
- **Filtro de Conteúdo:** Controle sobre o tipo de conteúdo acessado.
- **Alta Disponibilidade:** Garantia de funcionamento contínuo dos serviços.
- **Gerenciamento Centralizado:** Facilita a configuração e monitoramento da segurança.
- **Alertas e Logs:** Registro de eventos para análise e auditoria, em conformidade com o Marco Civil da Internet e a LGPD.

A aquisição se dará por meio de sistema de compra por licitação. Justifica-se pela necessidade de mantermos o funcionamento das camadas de segurança de nosso datacenter e provimento de internet por mais 5 anos, ampliando a capacidade de recursos.

As equipes responsáveis pela gestão de rede (CORED) e segurança (COCIB) do CIASC, já possuem amplo conhecimento da plataforma Fortinet existente, que já está em operação desde 2020, incluindo treinamento oficial do fabricante.

5. Estimativas das quantidades para contratação, acompanhadas de memórias de cálculo e dos documentos que lhe dão suporte (considerar interdependências com outras contratações, de modo a possibilitar economia de escala)

Foi realizada análise de atualização do parque mantendo a qualidade, compatibilidade e facilidade de gerenciamento, sem esquecer que se trata de um sistema de segurança de dados para toda a instituição, em suas áreas meio e fim do CIASC. O quantitativo foi definido utilizando como base o histórico de aquisição de anos anteriores, crescimento histórico do tráfego e margem de segurança (média de 30%). O quantitativo dos itens citados foi verificado pela equipe da GERED/COCIB/CORED junto à necessidade técnica da empresa, sempre buscando a melhor solução custo-benefício.

6. Levantamento mercadológico (que consiste na análise das alternativas possíveis, e justificativa técnica e econômica da escolha do tipo de solução a contratar) (art. 18, § 1º, V, da Lei Federal nº 14.133, de 2021).

Foi realizado levantamento de soluções baseados nos aspectos abaixo relacionados:

A) Disponibilidade de solução similar em outro órgão ou entidade da Administração Pública.

Em levantamento realizado na ferramenta de banco de preço https://pncp.gov.br/, foram identificadas algumas contratações dos últimos meses referentes às soluções FORTINET.

B) As alternativas do mercado:

Em 2020 foi realizado o PE CIASC **00001531/2020** onde o CIASC precisou conhecer as soluções disponíveis no mercado para Next Generation Firewalls (NGFW). Na época o processo licitatório deu como vencedor a FORTINET que continua sendo um dos melhores fabricantes, inclusive em diversos outros órgãos públicos. A atualização de licenças e novos equipamentos devem ser desta marca por uma questão de compatibilidade técnica para garantir a solução integrada. O mercado oferece diversas empresas que trabalham com o fabricante FORTINET. Desta forma, e levando-se em conta a recente estrutura montada nesta plataforma cujas licenças adquiridas vão até metade de 2026, não se cogitou a mudança para outro fabricante. Está hipótese traria retrabalho, novos treinamentos, e consequentemente maior tempo de implantação.

C) As necessidades de adequação do ambiente do CIASC e compatibilidade para viabilizar a execução contratual;

Deve-se manter a solução focada em “part numbers” dos referidos fabricantes, mantendo a total compatibilidade com a solução hora aplicada no CIASC, não haverá necessidades de adequação adicional do ambiente. A instalação se dará pela equipe do CIASC com o devido suporte padrão do fabricante. O serviço SD-WAN oferecido pelo CIASC dentro da solução Conectividade Integrada é baseado em equipamentos Fortinet Fortigate, e a manutenção de uma plataforma Fortinet no CIASC é fundamental para garantir a compatibilidade e funcionamento do SD-WAN. Ainda neste quesito, é importante ressaltar o custo financeiro e risco da mudança de plataforma de segurança para a instituição. No processo de aquisição de Firewalls realizado em 2020, foi necessário cotar um item de **suporte à migração e consultoria**, que gerou um **custo adicional de R$673.011,55** (item 4 do contrato).

D) A existência de softwares disponíveis e suas atualizações;

Não foram identificados softwares públicos para este tipo de soluções, visto que aquisição de hardware não é simplesmente substituído por software; e as soluções existentes de aplicações utilizadas na CIASC teriam custo de substituição sem garantias técnicas mínimas. Neste tipo de solução de firewall de grande porte e com todas essas funcionalidades integradas, nenhuma aplicação de softwares livres (freeware ou GPL) atenderia as necessidades.

E) Os diferentes modelos de contratação de prestação dos serviços;

1) Locação de equipamento

A locação ou prestação de serviços não foi considerada devido ao comprometimento das verbas de custeio do CIASC, já destinada para manutenção de serviços essenciais da instituição, como pessoal, limpeza, segurança etc.

Esta forma de contratação de soluções de TI, como a contratação na modalidade de serviço, onde a empresa contratada, mediante pagamentos na forma de mensalidade, prove o fornecimento da solução contratada.

Existem modos de fornecimento da solução de equipamentos como serviço:

• A modalidade onde o equipamento fica hospedado na nuvem da empresa contratada ou do fabricante, não havendo a presença física do equipamento na rede de dados do cliente, e todo o tráfego de internet da rede local é direcionada para a nuvem. Nesta modalidade o pagamento da mensalidade varia de acordo com a quantidade de tráfego que é inspecionado e processado na nuvem. Para este tipo de serviço existe a necessidade estudos mais profundos dos impactos técnicos na nossa rede, além de ficar a questão da compatibilidade com a infraestrutura atual.

• Existe a modalidade onde a empresa contratada realiza o fornecimento, instalação e configuração do equipamento físico na rede de dados do cliente, mediante o pagamento de um valor mensal fixo, ficando a empresa contratada responsável pela garantia, suporte e monitoramento do equipamento. Essa modalidade se assemelha a uma locação. Alguns equipamentos legados podem ficar contemplados num contrato com a empresa, desta forma a empresa precisaria conhecer bem nossa estrutura para assumir. O nível de acesso e segurança deve ser estudado e previsto, mas diversas empresas trabalham com este tipo de serviço. Em ambos os casos, o não pagamento do valor da mensalidade, em virtude de o equipamento não pertencer ao cliente, acarreta a suspensão da prestação do serviço e/ou remoção do equipamento e, sendo que os equipamentos são fundamentais no funcionamento e proteção da rede de dados, tal suspensão na prestação do serviço traria enormes prejuízos a

instituição deixando sua rede de dados e seus usuários sem proteção e expostos a ataques cibernéticos ou ainda sem acesso à Internet e sistemas hospedados no CIASC.

F) Verificação dos diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

Entende-se que a quantidade de fornecedores pode ser considerada restrita no caso do licenciamento, pois o projeto aponta para o mesmo fabricante, porém justifica-se que os requisitos são indispensáveis de compatibilidade. Conforme análise comparativa de soluções. (tópico 8)

7. Estimativa do valor da contratação (art. 18, § 1º, VI, da Lei Federal nº 14.133, de 2021).

O preço máximo estimado da contratação é de **R$ 6.500.000,00 (seis milhões e quinhentos mil reais).** O preço estimado foi obtido através de consulta direta ao fabricante Fortinet, que encaminhou ao parceiro fornecedor que poderá entregar a solução. Outros fornecedores do mesmo fabricante também poderão participar do processo licitatório. A viabilidade econômico-financeira do projeto visa retorno financeiro através de produtos desenhados pela GEDEM e GERED, como virtualização de servidores, circuitos de conexão à redes de governo e Internet, serviços de conectividade baseados em SD-WAN (CIASC Conectividade Integrada) e a venda de firewall como serviço,. Ela se justifica também pela importância para a continuidade da prestação dos serviços de rede, Data Center e VPN do CIASC.

8. Comparativo das soluções

Solução 1: Renovação das licenças FortiAnalyzer, Fortimanager, Firewall FG-3301E por mais 05 anos e Troca do firewall FG-2200E:

Característica	Firewalls de Datacenter (Licença Enterprise Premium - Renovação)	Firewalls de Provimento Internet (Licença UTP - Aquisição)

Objeto da Demanda	Renovação de licenças e suporte técnico para *firewalls* de Datacenter (3301E).	Aquisição de novo cluster de *firewalls* de provimento Internet com capacidade de tráfego ampliada.
Licença/Suporte	Fortinet **Enterprise Premium** por 5 anos, incluindo FortiCare Premium.	Licenças avançadas (**UTP - Unified Thread Protection**) e garantia de 5 anos.
Função Principal	Garantir a segurança cibernética dos serviços digitais hospedados nos Data Centers (tráfego Leste-Oeste).	Garantir o acesso seguro à Internet (tráfego Norte-Sul).
Capacidade do Hardware	Capacidade de *hardware* disponível para acomodar demandas atuais e futuras.	Necessita de substituição por equipamentos com **maior capacidade** de tráfego.
Componentes de Segurança (Geral)	Inclui os serviços UTP + serviços avançados como DLP (Data Loss Prevention), Inline CASB, Attack Surface Security e proteção para dispositivos IoT.	Inclui serviços de **Proteção contra Ameaças Unificada** (Intrusion Prevention, Antivírus, Application Control, Sandboxing baseado em nuvem, Web & DNS Filtering, Anti-spam).
FortiCare (Suporte)	**FortiCare Premium** (incluído no pacote Enterprise Premium).	**FortiCare Premium** (geralmente incluído no pacote UTP).

Prazo de Cobertura	5 anos.	5 anos.
Justificativa Específica	Encerramento da cobertura de suporte e garantia em junho de 2026, sendo necessária a renovação.	O cluster atual está operando próximo do limite de capacidade de tráfego, exigindo ampliação.

Complementando a atual situação:

Necessidade de Licenças e Suporte: As licenças e o suporte são essenciais para a atualização permanente de vulnerabilidades, respostas, tabelas de vírus detectáveis e atualizações de *software*.

Renovação x Aquisição: A renovação do cluster de Datacenter é justificada pelo vencimento do suporte, enquanto a aquisição de um novo cluster de provimento Internet se justifica pela necessidade de ampliação da capacidade de tráfego.

Previsão de Aquisição: A contratação efetiva dos equipamentos e licenças deve ocorrer até **01/03/2026**.

Contrato Anterior: Os *firewalls* existentes foram adquiridos em 2021, com licenças de suporte e garantia por 5 anos.

Solução 2: Renovação das licenças FortiAnalyzer e Fortimanager por mais 05 anos e Troca dos pares de firewalls FG-2200E e FG-3301E por um par de firewall que engloba os dois modelos, como por exemplo o FG-3200F:

É totalmente possível realizar a consolidação dos serviços de dois *clusters* de *firewall* (**FG-2200E** e **FG-3301E**) em um único *cluster* de alta performance como o **FG-3200F por exemplo.**.

Essa estratégia de consolidação em um modelo da Série F mais recente é um caminho lógico para o ETP, pois não só resolve a necessidade de **ampliação da capacidade de tráfego** para a o Data Center e a Internet, como também aprimora a infraestrutura do Datacenter, migrando de processadores NP6 (série E) para o mais potente NP7 (série F).

A tabela a seguir demonstra o ganho de desempenho com a migração para o FG-3200F.

CIASC
CENTRO DE INFORMÁTICA
E AUTOMAÇÃO DO ESTADO DE SANTA CATARINA S.A.

Comparativo de Consolidação: FG-2200E + FG-3301E vs. FG-3200F (sugerido)

Característica	Cluster Existente de Datacenter + Internet (FG-2200E + FG-3301E)	Novo Cluster Consolidado (FG-3200F)
Modelos	1 Cluster de 2 Firewalls FG-3301E (Datacenter) + 1 Cluster de 2 Firewalls FG-2200E (Provimento Internet)	1 Cluster de 2 Firewalls FG-3200F (Datacenter + Internet)
Processador SPU	SPU NP6 / CP9	**SPU NP7** / CP9 (Tecnologia de hiperescala)
Firewall Throughput (Total)	160 Gbps(3301E) + 158 Gbps (2200E) =318 Gbps	**387 Gbps** (Ganho de 21% em velocidade bruta de firewall)
Threat Protection Throughput*	17 Gbps(3301E) + 11 Gbps(2200E) = 28 Gbps	**45 Gbps** (Ganho de 60.7% em proteção de ameaças)
SSL Inspection Throughput	21 Gbps(3301E) + 17 Gbps (2200E) = 38 Gbps	**29 Gbps** (Pode indicar necessidade de **otimização** na inspeção SSL)
New Sessions/Second (CPS)	$460.000 CPS (3301E) + 500.000 CPS (2200E) = 960.000 CPS	**800.000 CPS**
Concurrent Sessions (Total)	50 Milhões (3301E)+ 24 Milhões (2200E) = 74 Milhões	**70 Milhões** (Capacidade similar)

Interfaces de Alta Velocidade (Max)	40 GbE	**400 GE** (QSFP-DD), 200 GE, 100 GE
Armazenamento Onboard	FG-3301E tem 2x 1 TB SSD, FG-2200E não tem (0)	2x 1 TB SSD

**Threat Protection Throughput é a métrica mais relevante, pois representa o desempenho do firewall com as funções de segurança (IPS, AV, App Control) ativadas, que é o cenário de uso real.*

(Análise da Consolidação):

Aspecto	**Avaliação da Consolidação para FG-3200F**
Aumento de Capacidade	**Positivo**. O FG-3200F entrega um aumento significativo no *Threat Protection Throughput* (60.7% de ganho), atendendo diretamente à demanda por **capacidade de tráfego ampliada**.
Desempenho Geral	**Misto**. Embora o desempenho de Firewall e *Threat Protection* aumente, o FG-3200F apresenta uma **redução** na taxa máxima de *New Sessions per Second* e uma capacidade ligeiramente menor de *Concurrent Sessions* e *SSL Inspection* quando comparado ao **somatório** dos dois modelos antigos.
Risco Técnico	A consolidação reduz a resiliência física (de 2 *clusters* separados para 1 *cluster* único) e pode criar um **ponto único de falha lógica** para ambos os serviços (Datacenter e Internet), embora o FG-3200F suporte *clustering* HA (Alta Disponibilidade).
Licenciamento	Unificação do licenciamento de ambas os equipamentos (FG-2200E + FG-3301E) gerando economia na contratação do suporte e atualizações.

9. Descrição da solução escolhida (art. 18, § 1º, VII, da Lei Federal nº 14.133, de 2021)

A solução escolhida para cada um dos itens do edital busca resolver um objetivo específico de melhoria da infraestrutura da segurança de rede do CIASC. São ações distintas pois envolvem objetos distintos, mas se integram na solução total.

A solução escolhida foi:

· **Solução 02** – Licitação para aquisição de equipamentos novos e renovação de licenciamento, através de procedimento de compra de equipamentos de firewall para provimento e datacenter, seguindo o padrão estabelecido dentro do CIASC.

A licitação de compra garante a aplicação dos recursos financeiros já pré estabelecidos, e quando a equipe técnica tiver oportunidade de trabalhar as mudanças de equipamentos. Pode-se dividir em graus de urgência os itens deste lote:

A) Urgente: Substituir os pares de equipamentos do modelo FG-2200E e FG-3301E, pois implica em risco a segurança de rede, onde as licenças necessárias perderão funcionalidades e um par dos equipamentos está chegando no limite de sua capacidade operacional.

B) Urgente: a aquisição do licenciamento do FortiAnalyzer que é a ferramenta de gestão de logs da solução de segurança atual, que ficará sem suporte e garantia do fabricante a partir de 26/06/2026;

C) Urgente: a aquisição do licenciamento do FortiManager que é a ferramenta de sincronização e gerência da solução de segurança atual, que ficará sem suporte e garantia do fabricante a partir de 26/06/2026;

10. Justificativas para o parcelamento ou não da contratação (art. 18, § 1º, VIII, da Lei Federal nº 14.133, de 2021)

A aquisição da nova solução de firewalls deve ser realizada integralmente, em parcela única, devido à natureza interdependente dos requisitos técnicos. O parcelamento comprometeria a compatibilidade, a alta disponibilidade e a eficiência do gerenciamento, introduzindo riscos operacionais e dificultando a integração com a infraestrutura existente. A contratação coesa e unificada é essencial para garantir a segurança contínua das aplicações governamentais e o acesso seguro à internet, otimizando o desempenho e a proteção contra ameaças, conforme os objetivos do CIASC.

11. Contratações correlatas e/ou interdependentes (art. 18, § 1º, XI, da Lei Federal nº 14.133, de 2021)

O Credenciamento 021/2025 (SGPE CIASC 1574/2024) prevê que as empresas credenciadas forneçam firewalls Fortinet de menor porte para instalação localmente nos clientes contratantes que sejam compatíveis com os firewalls existentes no CIASC. Deste modo, para garantir o funcionamento do serviço designado “SD-WAN”, é necessário manter firewalls Fortinet disponíveis no CIASC.

12. Providências a serem adotadas pela Administração previamente à celebração do contrato (art. 18, § 1º, X, da Lei Federal nº 14.133, de 2021)

Não há necessidade de adoção de outras ações adicionais para que esta contratação, pois as licenças e equipamentos estão sendo solicitados com suporte adequado e configuração do ambiente se dará em conjunto pela equipe técnica do CIASC e da CONTRATADA.

Foram mapeados e levados em consideração os possíveis riscos e as medidas para tratamento caso ocorram. O mapa de riscos está presente neste processo.

13. Possíveis impactos ambientais e respectivas medidas mitigadoras (art. 18, § 1º, XII, da Lei Federal nº 14.133, de 2021)

Existem impactos ambientais em caso de descartes inadequados no futuro, porém em se tratando de material patrimoniável do CIASC, todo descarte é realizado por meio do almoxarifado responsável, conforme legislação vigente.

14. Resultados pretendidos (*art. 18, § 1º, IX, da Lei Federal nº 14.133, de 2021)*

O CIASC disponibiliza de uma infraestrutura de TI para todos os sistemas do Governo Estaduais, algumas Prefeituras, e Tribunais. A instituição como um todo se beneficia direta e indiretamente com a aquisição pretendida, pois garante que a Empresa preste serviços de qualidade à sociedade, bem como atenda as próprias necessidades institucionais, seguindo princípios de confiabilidade, integridade e disponibilidade. Neste contexto, os serviços de Tecnologia da Informação, tem um papel importante para manter estas metas e objetivos, que a GERED busca cumprir.

Tecnicamente, a atual a solução da FORTINET, permite um nível de segurança a filtragem de pacotes, aplicando regras de bloqueios nas camadas de rede e

transporte do modelo OSI, Filtro de Botnet, Gateway (Antivírus, Anti-Spyware, Prevenção de Intrusão), filtro de conteúdo, possibilidade de atualização de software e firmware, alta disponibilidade, gerenciamento centralizado das configurações, alertas e Logs. A nova solução irá renovar e ampliar a capacidade da atual solução.

Está realidade atende as boas práticas de tecnologia no que diz respeito a segurança dos dados e gerenciamento da rede, além de garantir aderência às melhores práticas nacionais e internacionais da área de Segurança da Informação, e em consonância com as normas vigentes.

Os resultados desejados são objetivamente:

1) Atualizar as licenças da solução de segurança:

A maioria das licenças atuais tem prazo final previsto para metade de 2026, portanto precisamos adquirir novas licenças para manter a segurança da instituição. É desejado manter os serviços de controle de usuários locais e remotos, logs etc.

A segurança dos dados pessoais e da instituição é importante e protegida por legislação específica (LGPD), sendo está mais uma ferramenta para auxiliar neste propósito.

2) Adquirir equipamentos:

Dois dos equipamentos existentes estão no limite da capacidade e precisamos adquirir substitutos, e adquirir equipamentos de melhor performance.

15. Posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina (art. 18, § 1º, XIII, da Lei Federal nº 14.133, de 2021)

Justificativa técnica da escolha da solução:

Tecnicamente a solução tem as seguintes vantagens:

· total compatibilidade

. longevidade (equipamentos de maior porte)

. alta disponibilidade

. solução conhecida da equipe de TI;

. monitoramento e rastreabilidade das atividades de rede;

. fornecimento de relatórios das atividades de rede;

. atende as necessidades do CIASC

Complemento com informações de conhecimento público:

A Tecnologia da Informação e Comunicação (TIC) tornou-se ferramenta fundamental para a execução dos serviços nos setores público e privado. Especialmente no setor público, praticamente todos os processos de trabalho já operam, diretamente ou indiretamente, com sistemas de informação. Deste modo, tais meios são amplamente disseminados e utilizados na execução das atividades administrativas, operacionais do CIASC.

Como peculiaridade marcante, os meios de TIC sofre rápido processo de obsolescência e desgaste naturais, seja por conta do tempo de uso ou pelo aumento dos recursos computacionais ofertados na instituição, que impõem aos gestores a adoção de medidas que garantam a continuidade do exercício permanente de suas atribuições institucionais. A continuidade dos serviços é um dos principais atributos a ser levado em consideração pelos gestores, tendo em vista que a interrupção da prestação dos serviços públicos causa indesejáveis prejuízos à sociedade.

A solução de segurança atualmente em uso é o principal ativo de segurança da informação, sendo o responsável pela inspeção do tráfego da rede interna/externa de toda a Universidade. A aquisição de um novo equipamento de firewall visa manter a continuidade dos serviços fornecendo alta disponibilidade, integridade e confidencialidade em seus sistemas de informação hospedados no Data Center do CIASC.

As novas técnicas de invasão e captura de informações, por parte de pessoas e grupos mal intencionados, estão se tornando cada vez mais comuns na rede mundial de computadores. Assim, o CIASC precisa estar sempre atualizada e preparada tecnicamente para enfrentar essas tentativas de captura de dados, tanto de forma ostensiva, quanto preventiva, para manter e prover políticas de segurança da informação personalizadas para: usuários, grupos de usuários, servidores, estações de trabalho, portas, protocolos e aplicações. Permitindo a continuação dos serviços oferecidos pela Empresa Pública.

16. Vantajosidade comercial da contratação.

Em pesquisa de preços realizada no Portal Nacional de Contratações Públicas, foi possível identificar pregões com itens semelhantes, com características técnicas parecidas ao caso do CIASC, conforme a equipe da Coordenação de Cibersegurança analisou. Para calcular o preço de referência, foi realizada uma pesquisa com

fornecedores da respectiva solução e planilhado os valores obtidos conforme metodologia orientada pela COLIC do CIASC. Apesar da escolha ser a solução de maior custo em hardware e software, ela é no nosso entendimento a solução de melhor qualidade, longevidade, fornecendo ganhos indiretos com o gerenciamento e funcionalidades. Ganhos estes difíceis de mensurar em termos de valores monetários. A viabilidade econômica foi discutida com a administração que considerou possível de ser realizada.

Justificativa da Viabilidade:

Esta equipe de planejamento entende existir razoabilidade suficiente para esta aquisição, pois consideramos necessária para o CIASC, sendo a solução escolhida mais adequada pelos motivos apontados.

Consideramos que dentre todas as soluções a aquisição de um par de equipamentos em alta disponibilidade com a total compatibilidade com a solução existente; é a que apresenta as melhores vantagens, menores riscos; facilita o trabalho da equipe de TI e diminui o tempo de parada da rede do CIASC; e por fim, garante o atendimento em todos as áreas.

Após a análise das alternativas de atendimento das necessidades elencadas, conclui-se pela VIABILIDADE DA CONTRATAÇÃO, uma vez considerado o potencial benefício e, em termos de eficácia, efetividade e economicidade.

Pelo exposto já citado em tela, RECOMENDAMOS o prosseguimento da pretensão contratual.