# ESTUDO TÉCNICO PRELIMINAR - ETP

## 1. Informações Básicas

Número do processo: P378488/2025.

## 2. Descrição da necessidade da contratação

Este documento visa justificar a contratação de uma solução de firewall para a infraestrutura de TI da PMS, garantindo a continuidade dos serviços prestados. A proposta segue as melhores práticas de segurança da informação, além de viabilizar a centralização da gestão e substituir o firewall atual, cuja licença está prestes a expirar.

Atualmente, a infraestrutura de TI conta com 2 (dois) servidores físicos executando a solução de firewall **SOPHOS** em alta disponibilidade. Esses firewalls desempenham um papel crítico na segurança da rede, sendo responsáveis por gerenciar as regras de controle de acesso à internet, prevenir ataques cibernéticos, bloquear acessos não autorizados, inspecionar tráfego em tempo real e garantir a integridade e a disponibilidade dos serviços.

solução adquirida em 2021 foi implementada com o propósito de proteger todo o tráfego de rede, abrangendo todos os ativos da Prefeitura. No entanto, com o crescimento da demanda ao longo do tempo, a capacidade do equipamento tornou-se insuficiente para suportar a carga atual, exigindo a adoção de ajustes técnicos e a descentralização da gestão para outras soluções de controle de conteúdo e firewall. Além disso, o equipamento foi descontinuado pelo fabricante, impossibilitando a renovação da licença, que tem vencimento previsto para **31/03/2025.**

- **As consequências da não contratação da licença e serviço necessários incluem:**
  - Descontinuidade no padrão adotado para o controle de conteúdo de acesso à internet;
  - Possíveis dificuldades de acesso a sites e serviços devido à complexidade de manter a gerência da rede descentralizada;
  - Aumento de vulnerabilidades e exposição a ataques cibernéticos;
  - Redução do desempenho da rede devido à falta de otimização e proteção centralizada.

A Lei 14.133/2021, que estabelece o novo regime de licitações e contratos administrativos, exige a elaboração do Documento de Formalização

da Demanda (DFD) para justificar a necessidade da contratação. A contratação de uma nova solução de firewall é essencial para **garantir a segurança, disponibilidade e integridade da rede da Prefeitura.** O atual equipamento não atende mais à demanda crescente, exigindo ajustes técnicos que descentralizam a gestão da segurança, aumentando a complexidade operacional. Além disso, sua descontinuidade pelo fabricante impede a renovação da licença, que expira em 31/03/2025. A ausência de uma solução robusta compromete a proteção contra ameaças cibernéticas, o controle de acesso e a continuidade dos serviços críticos, tornando indispensável a aquisição de um novo firewall adequado às necessidades atuais e futuras da infraestrutura de TI.

- **Benefícios da Contratação**

A contratação do serviço de suporte técnico do fabricante trará os seguintes benefícios para a PMS:

**a) Segurança Reforçada**

Proteção avançada contra ataques cibernéticos, malwares e acessos não autorizados.

**b) Gestão Centralizada**

Facilidade na administração das regras de segurança e controle de acesso em um único ambiente.

**c) Melhor Desempenho**

Capacidade de suportar o tráfego crescente sem comprometer a disponibilidade da rede.

**d) Atualizações e Suporte**

Garantia de suporte técnico e atualizações regulares do fabricante, reduzindo vulnerabilidades.

**e) Alta Disponibilidade**

Redundância e continuidade dos serviços, evitando falhas e interrupções na conectividade.

**f) Conformidade com Normas**

Atendimento a requisitos de segurança da informação e políticas institucionais.

**g) Otimização do Controle de Acesso**

Gerenciamento eficiente do uso da internet e das aplicações dentro da rede.

Diante do exposto, a contratação e implementação dos itens descritos são fundamentais para garantir a continuidade, segurança e a qualidade dos serviços públicos prestados pela Prefeitura Municipal de Sobral. A contratação de uma nova solução de firewall é uma medida estratégica e indispensável para a continuidade da segurança e estabilidade da infraestrutura de TI da Prefeitura. Com o aumento da demanda e a descontinuidade do equipamento atual, é fundamental investir em uma solução moderna, robusta e escalável, capaz de garantir a proteção eficaz da rede e a continuidade dos serviços essenciais. Além disso, a nova solução permitirá a centralização da gestão de segurança, otimizando processos e reduzindo riscos operacionais. A adoção dessa medida assegurará que a Prefeitura mantenha um ambiente seguro, conforme as melhores práticas e requisitos de segurança da informação. Portanto, justifica o preenchimento do Estudo Técnico Preliminar, em atendimento ao disposto na Lei 14.133/2021.

## 2.1. Previsão no plano de contratações anual

A aquisição em apreço não se encontra prevista no PCA- 2025 da SESEP, porém foi identificada a necessidade de incluir o referido serviço a ser contratado.

## 3. Área requisitante

| SETOR REQUISITANTE | RESPONSÁVEL PELO SETOR |
|---|---|
| Coordenação de Gestão Estratégica de Tecnologia da Informação | Nome: Hugo Firmino Damasceno<br>Matrícula: 48745<br>E-mail: hugofirmino@sobral.ce.gov.br<br>Telefone: (88) 9.9659-5679 |

## 4. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.2. Natureza: serviços e fornecimentos contínuos.

4.2.1. Devido às características da rede de computadores do Município, a solução de segurança deve ser do tipo virtual, ou seja, deve ser composta por software projetado e dimensionados especificamente para analisar e suportar grandes volumes de tráfegos, que permitam a implementação de diversos recursos de segurança.

4.2.2. Desta forma, deve ser do tipo Next Generation Firewall (Firewall de nova geração) devendo ser capaz de realizar reconhecimento de aplicações e de usuários, auxiliar na prevenção de ameaças e no controle de permissões e políticas de acesso com maior granularidade.

4.2.3. Tais exigências são justificáveis tendo em vista o risco da exposição indevida de informações ou de ataques que reduzam a disponibilidade de sistemas. Desta forma a solução deverá permitir a verificação do comportamento do tráfego em tempo real, identificando acessos abusivos ou indevidos que podem caracterizar tentativas de invasão aos ambientes digitais do Município, coleta de dados ou simplesmente tentativas de derrubada dos serviços digitais.

4.2.4. Deverá fazer parte da composição da solução a elaboração de projeto de instalação e configuração de modo a possibilitar a análise prévia da equipe técnica do Município quanto aos procedimentos necessários para a implementação da solução, com o planejamento de janelas de indisponibilidades e plano de comunicação de modo a dar maior transparência do processo para os usuários da rede.

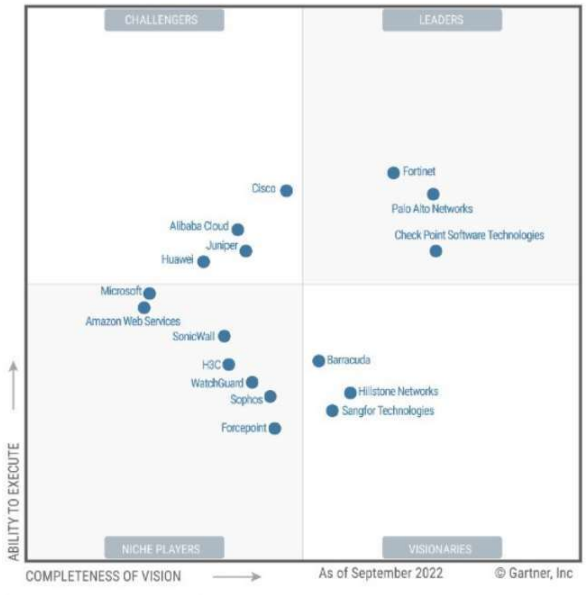
4.2.5. Todos os serviços de instalação e configuração deverão ser executados pela CONTRATADA, de modo a não sobrecarregar a equipe de servidores e colaboradores do Município, porém as atividades deverão ser acompanhadas pelos servidores e colaboradores que atuarão na operação da solução após entregue pela CONTRATADA.

4.2.6. A solução deverá ter ainda em sua composição um item para treinamento, para garantir que ocorra a transferência do conhecimento para os servidores e colaboradores que atuam na infraestrutura de TI do Município.

4.2.7. De modo a tornar viável o investimento sem riscos da continuidade dos serviços e com garantia de atualização de softwares e componentes da solução, será exigido garantia, assistência técnica e suporte técnico por período não inferior a 60 meses, em regime 24x7.

4.2.8. Sobre o atual mercado, o quadrante Gartner traz as seguintes referências para essas soluções, que abarcam as necessidades almejadas:

**Figure 1: Magic Quadrant for Network Firewalls**




Source: Gartner (December 2022)

4.2.9. Das necessidades que pretende-se manter e evoluir, e elencando a análise de soluções e a seleção da opção mais adequada para atingir esses fins organizacionais, cita-se as abaixo:

a) Proteção das informações sensíveis;

b) Aumentar a eficiência da segurança, proteção e autenticidade dos dados e acessos;

c) Redução da probabilidade de ocorrência de incidentes de segurança;

d) Controle da saída de dados sensíveis, seja via transferência de arquivos ou publicação em páginas da internet;

e) Amplificação da camada de proteção e visibilidade de informações sensíveis;

f) Fluxo automatizado de descoberta de informações sensíveis em todos os pontos do ambiente;

g) Incrementar e otimizar o gerenciamento, a eficiência e a proteção das informações do ambiente tecnológico;

h) Melhoramento da capacidade de detecção e prevenção de ameaças cibernéticas, comportamentos suspeitos dos usuários, mal-uso dos dados institucionais e vazamentos de dados sensíveis;

i) Atualização e modernização do ambiente tecnológico do Município, mantendo assim a infraestrutura de rede segura, disponível e plenamente operacional para a disponibilidade de informações precisas e confiáveis à sociedade e aos diversos usuários de seus sistemas;

j) Manutenção da integridade, confiabilidade e segurança do ambiente tecnológico, bem como disponibilizar equipamentos, bases de dados e informações precisas e confiáveis.

## 5. NECESSIDADES TECNOLÓGICAS

5.1. Para assegurar a continuidade dos serviços e evitar que falhas em um único equipamento provoquem indisponibilidade, a solução deverá ser baseada em software com suporte a alta disponibilidade. O mecanismo de failover entre os ambientes ativo e passivo deverá ocorrer de forma automática, incluindo o failback, garantindo a retomada segura e transparente da operação.

5.1.1. Durante a vigência contratual e o prazo de garantia, o fabricante deve garantir a atualização de patches e softwares de todos os componentes que compõe a solução de TIC, de modo irrestrito e ilimitado.

5.1.2. A solução deve ser oferecida na última versão disponibilizada pelo fabricante. Na data da proposta, nenhum dos softwares componentes da solução de proteção ofertados poderão estar listados pelo fabricante com data definida para fim de suporte (“end of support”) ou fim de vendas (“end of sale”).

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

6.1. Além das necessidades de negócio e tecnológicas, a presente contratação destaca aqueles requisitos que devem ser considerados ao longo do planejamento da contratação para assegurar o alcance dos objetivos pretendidos com a contratação, conforme a seguir:

**6.2. Requisitos de Negócio**

6.2.1. Manutenção da integridade, confiabilidade e segurança do ambiente tecnológico, bem como disponibilizar equipamentos, bases de dados e informações precisas e confiáveis.

6.2.2. Incrementar e otimizar o gerenciamento, a eficiência e a proteção das informações do ambiente tecnológico.

6.2.3. Aprimoramento continuado das ações de Segurança da Informação, objetivando o atendimento à totalidade dos usuários do ambiente tecnológico.

6.2.4. Melhoramento da capacidade de detecção e prevenção de ameaças cibernéticas, comportamentos suspeitos dos usuários, mal-uso dos dados institucionais e vazamentos de dados sensíveis.

6.2.5. Atualização e modernização do ambiente tecnológico, mantendo assim a infraestrutura de rede segura, disponível e plenamente operacional para a disponibilidade de informações precisas e confiáveis à sociedade e aos diversos usuários de seus sistemas.

**6.3. Requisitos de Capacitação**

6.3.1. Na elaboração do Projeto Executivo deverá ser detalhado e especificado o treinamento a ser ministrado pela contratada, com o mínimo de 20h, devendo ser gravado, podendo ser realizado de forma remota, para não interromper as atividades da equipe técnica do Município.

**6.5. Requisitos de Manutenção**

6.5.1. O serviço de manutenção, atualização e suporte técnico da solução deverá ser executado pela Contratada e /ou pelo Fabricante durante toda a vigência contratual, a partir da data de emissão do Termo de Recebimento Definitivo referente à implantação e operacionalização da solução no ambiente tecnológico do Município, e deverá contemplar obrigatoriamente no mínimo:

a) Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;

b) Atualização dos softwares fornecidos se houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos;

c) Correções de falhas (bugs) de software durante o período contratual, sendo executadas pela Contratada e /ou pelo Fabricante da solução, sem ônus adicionais;

d) Execução de teste gerais de funcionamento e conectividade;

e) Execução de configuração de rede e roteamento para as aplicações configuradas;

f) Execução de cópia de segurança (backup) das configurações dos equipamentos;

g) Entrega, por parte da Contratada, de manuais técnicos e/ou documentação dos softwares licenciados em caso de alterações dos mesmos, sem ônus adicionais para o CONTRATANTE.

6.5.2. As novas versões do objeto contratado deverão ser disponibilizadas em até 5 (cinco) dias corridos, a partir do lançamento oficial da versão.

6.5.3. Caso os serviços de manutenção e suporte técnico não sejam executados diretamente pela Contratada, mas sim pelo próprio Fabricante ou por empresa(s) representante(s) ou credenciada(s) por este, a Contratada deverá comunicar tal fato a CONTRATANTE, e assegurar que todos os padrões de atendimento e demais requisitos contratuais serão cumpridos. O aceite por parte do CONTRATANTE do atendimento não exime a Contratada da responsabilidade integral pelo atendimento e cumprimento dos prazos acordados.

**6.6. Requisitos Temporais**

6.6.1. O prazo de vigência do contrato será de 5 (cinco) anos, contados a partir da data da sua assinatura, podendo ser prorrogado, respeitada a vigência máxima decenal, desde que haja preços e condições mais vantajosas para a Administração, nos termos dos artigos 106 e 107 da Lei 14.133/2021.

6.6.2. A reunião inicial de alinhamento com a Contratada, deverá ocorrer em no máximo 10 (dez) dias corridos, posteriormente à assinatura do instrumento contratual.

6.6.3. Os serviços de fornecimento do objeto – isto é, a execução completa dos serviços e tarefas previstas objetivando a plena e efetiva operacionalização da solução no ambiente do Município – deverão ser executados no prazo máximo de até 120 (cento e vinte) dias consecutivos a partir da assinatura da Ordem de Fornecimento ou Ordem de Serviço.

**6.7. Requisitos de Segurança e Privacidade**

6.7.1. A Contratada deverá conhecer todas as normas, políticas e procedimentos de segurança estabelecidos pelo Município para execução do Contrato.

6.7.2. A Contratada deverá assinar Termo de Ciência e Termo de Confidencialidade e Sigilo.

6.7.3. Não será permitido, salvo justificado, que o ambiente seguro seja acessado por pessoas além daquelas necessárias para a prestação de serviços do objeto contratado.

6.7.4. O acesso dos profissionais da Contratada às dependências do ambiente tecnológico estará sujeito às suas normas referentes à identificação (crachá funcional), trajes, trânsito e permanência em suas dependências.

**6.8. Requisitos de Arquitetura Tecnológicas**

6.8.1. Durante a implantação da solução, a Contratada deverá realizar, entre outras atividades: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, tunning, resolução de problemas e implementação de segurança.

6.8.2. Caberá à Contratada a disponibilização de todos os recursos necessários, tais como hardwares, softwares, recursos humanos necessários à instalação da solução.

6.8.3. Caberá à Contratada a disponibilização de ferramentas/scripts de retorno imediato ao estado original da estrutura da Contratada caso a instalação e migração dos produtos /softwares da Contratada apresente falha.

6.8.4. A Contratada realizará adequação/configuração da solução fornecida ao longo da etapa de migração e realização de novas configurações.

6.8.5. A Contratada deverá fornecer todas as licenças necessárias de todos os componentes da solução ofertada e dos elementos adicionais que se fizerem necessários à instalação/migração e à perfeita operação do ambiente de produção.

**6.9. Requisitos de Projeto e de Implementação**

6.9.1. A solução de TIC deverá ser plenamente implementada pela Contratada em no máximo 120 (cento e vinte) dias corridos, a partir da assinatura da Ordem de Serviço.

6.9.2. Em caso de alterações necessárias nas especificações do projeto original durante a execução dos trabalhos, competirá à Contratada elaborar o projeto da parte a ser alterada e submetê-lo à aprovação do Fiscal, não podendo ocorrer, no entanto, alteração substancial das disposições gerais formuladas pelo projeto original.

**6.10. Requisitos de Implantação**

6.10.1. Caberá à Contratada o irrestrito cumprimento das seguintes prerrogativas:

a) Responsabilizar-se pela completa implantação do projeto, ou seja, todos os custos necessários à operacionalização dos equipamentos;

b) Responsabilizar-se por todos os instrumentais necessários durante o período de implantação e testes de aceitação;

c) Instalar e configurar todos os produtos do fornecimento da solução;

d) Executar a integração de todos os produtos da solução, de modo a não prejudicar as atividades mantidas nos locais, podendo ser exigida a realização de algumas fases em horários noturnos e fins de semana para que seja cumprido o cronograma de entrega;

e) Elaborar a "Documentação e Finalização do Projeto", que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e/ou gerencial.

**6.11. Requisitos de Garantia e Manutenção**

6.11.1. O prazo de garantia dos serviços, que não envolvam reposição de componentes ou dispositivos, será de 90 (noventa) dias. Caso o serviço tenha que ser refeito dentro deste período, o ônus correrá por conta da Contratada.

6.11.2. O direito do CONTRATANTE à garantia técnica cessará caso a solução seja alterada pelo próprio ou por fornecedores que não a Contratada e/ou Fabricante responsável pelo serviço em questão.

6.11.3. Os itens que compõe a solução deverão ter garantia durante toda a vigência contratual.

6.11.4. O acesso para downloads de patches, drivers e quaisquer outras atualizações e/ou correções necessárias devem estar disponíveis 24x7 (vinte e quatro horas por dia, sete dias por semana), durante todo o período de garantia técnica, e podem ser feitos através de http ou ftp, no sítio do fabricante da solução.

**6.12. Requisitos de Experiência Profissional**

6.12.1. Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, que comprovem que a licitante já prestou serviços compatíveis em prazo e complexidade com o objeto desta contratação.

**6.13. Requisitos de Formação da Equipe**

6.13.1. A contratada deverá apresentar, em até 30 (trinta) dias após a assinatura do contrato, pelo menos um técnico certificado na solução proposta.

**6.14. Requisitos de Metodologia de Trabalho**

6.14.1. A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante.

6.14.2. A OS indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.

6.14.3. A CONTRATADA deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica e via telefônica.

**7. Levantamento de Mercado**

7.1. O objetivo deste levantamento é identificar e analisar as alternativas disponíveis para auxiliar a COTEC, autarquia da Prefeitura Municipal de Sobral na execução dos serviços objeto deste ETP, além de justificar a escolha da solução mais adequada.

7.2. Em análise ao mercado, foram realizadas consultas no Portal Nacional de Contratações Públicas, Portal de Licitações dos Municípios no site do Tribunal de Contas do Estado do Ceará – TCE, contratações anteriores do mesmo órgão, Portais de Transparências de outros órgãos e em outros sítios na internet, e identificamos 02 (duas) alternativas que podem suprir a necessidade, vejamos:

Para atender a necessidade da presente contratação foram encontradas as seguintes soluções possíveis:

**a)** Realizar um processo licitatório específico para a contratação de solução de segurança de perímetro, com aquisição individualizada de equipamentos e licenças, o que exigiria o desenvolvimento de especificações técnicas detalhadas, bem como a seleção de uma

empresa que atue no fornecimento e implantação da solução de firewall de última geração (Next Generation Firewall – NGFW).

**b)** Realizar a adesão a Ata de Registro de Preços já formalizada por outro ente da Administração Pública, visando à contratação de empresa especializada que forneça a solução completa de segurança perimetral (Firewall Next Generation), incluindo licenciamento de software, suporte técnico, atualizações automáticas e integração com o ambiente tecnológico existente na COTEC.

A alternativa **"a"**, apesar de possível, apresenta riscos operacionais e administrativos consideráveis. A elaboração de um edital para contratação direta desse tipo de solução exige profundo conhecimento técnico, atualização constante sobre as novas ameaças cibernéticas e grande nível de detalhamento nas especificações, o que pode gerar margens de interpretação e falhas no processo. Além disso, o pregão eletrônico pode ser moroso e envolver múltiplas etapas burocráticas (elaboração e publicação do edital, sessão pública, julgamento, habilitação, recursos e homologação), somadas ao risco de **licitação deserta** ou **fracassada**, que comprometeria a continuidade e a integridade da rede institucional. Outro ponto crítico é a imprevisibilidade dos valores praticados no certame, pois os preços estão sujeitos à dinâmica da concorrência no momento da licitação, podendo superar os valores já pactuados em atas vigentes e homologadas por órgãos públicos com maior poder de negociação.

Por sua vez, a alternativa **"b"** representa a solução mais eficiente e vantajosa sob os aspectos técnico, operacional e econômico. A adesão à Ata de Registro de Preços viabiliza a contratação imediata de uma empresa com expertise comprovada na entrega de soluções de segurança cibernética, garantindo que a COTEC disponha de um sistema de proteção robusto, escalável e compatível com os requisitos modernos de defesa digital. A utilização de um firewall de última geração (Next Generation Firewall) possibilita a aplicação de políticas avançadas de controle, filtragem de tráfego, inspeção profunda de pacotes (DPI), bloqueio proativo de ameaças, gerenciamento centralizado e geração de relatórios e indicadores que subsidiarão a tomada de decisão da equipe de TI. Além disso, ao aderir a uma ata vigente, a COTEC assegura um processo mais célere, com economia de recursos humanos, segurança jurídica e maior previsibilidade orçamentária. Cabe destacar ainda que essa abordagem evita a dependência de múltiplos fornecedores, centraliza o suporte técnico em um único prestador, e permite rápida substituição ou ampliação da solução, caso necessário. Por se tratar de uma tecnologia crítica para a proteção dos dados institucionais, a agilidade na contratação e a confiabilidade do fornecedor são fatores determinantes para a continuidade das operações da COTEC.

A escolha pela adesão à presente Ata de Registro de Preços foi motivada pelo fato de ela se destacar como a alternativa mais vantajosa sob os aspectos de economicidade, eficiência operacional e logística de implantação, especialmente no cenário atual, conforme demonstrado em pesquisa de mercado abrangente.

Além de atender plenamente aos requisitos técnicos e econômicos exigidos para a proteção da infraestrutura de rede da COTEC, essa alternativa também promove o princípio da celeridade administrativa, fundamental neste contexto. A adesão à referida ARP possibilita uma resposta rápida e segura às necessidades institucionais, evitando os entraves típicos de

um processo licitatório convencional, que exige maior tempo de tramitação e gera custos administrativos adicionais.

Dessa forma, conclui-se que a escolha da **alternativa "b"**, ao considerar a solução integrada de segurança perimetral por meio de Firewall Next Generation, representa a opção mais vantajosa para a Administração. A decisão está amparada na análise das relações custo-benefício, que evidenciam ganhos diretos e indiretos para a CONTEC, sobretudo pela agilidade na implantação da solução, centralização do suporte técnico, atualizações constantes e maior controle sobre o ambiente de rede.

É importante destacar que há, no mercado, diversas empresas capacitadas a fornecer soluções de segurança da informação com as especificações técnicas exigidas, o que demonstra a competitividade do setor e reforça a validade da adesão à ata, cujos preços e condições foram firmados com base em ampla concorrência.

Portanto, a presente adesão se configura como a alternativa mais eficiente, segura e economicamente justificada, permitindo à COTEC dispor de uma solução moderna, escalável e alinhada às boas práticas de segurança cibernética no setor público.

### 7.3. Justificativa da escolha da solução

A escolha da solução deve considerar não apenas os custos imediatos, mas também o potencial de eficiência e economia a médio e longo prazo, além da garantia de suporte técnico especializado e da capacidade de adaptação às exigências específicas da CONTEC, autarquia da Prefeitura do Município de Sobral/CE.

Após análise criteriosa das alternativas disponíveis, a solução mais recomendada é a **alternativa "b"**, que prevê a adesão à Ata de Registro de Preços para contratação de uma solução integrada de segurança de perímetro por meio de **Firewall Next Generation**, com fornecimento de licenças de software, suporte técnico contínuo, atualizações automáticas e sistema de gerenciamento centralizado. Essa alternativa se destaca por ser a solução mais completa, segura e viável para atender às necessidades tecnológicas da CONTEC, no que se refere à proteção da infraestrutura de rede e à garantia da integridade dos dados institucionais. Além disso, possibilita maior agilidade na contratação e na implantação da solução, reduzindo riscos operacionais e assegurando alinhamento com os princípios da eficiência, economicidade e celeridade administrativa.

### 7.4. Alternativas para a regularização da contratação

É importante salientar que o procedimento utilizado para regularização desta contratação e para justificar a contratação dos serviços pode ser entre através de Pregão Eletrônico ou uma Adesão à Ata de Registro de Preços vigente.

## 8. Estimativa das quantidades a serem contratadas

8.1. A estimativa das quantidades foi elaborada com base nas necessidades contínuas do Saae de Sobral, garantindo conformidade com a legislação e eficiência na execução contratual e consecução do interesse público envolvido, conforme a seguir:

| ITEM | DESCRIÇÃO | UNIDADE DE MEDIDA | QUANTIDADE |
|---|---|---|---|
| 1 | Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo A. | Und. | 1 |
| 2 | Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo A. | Und. | 1 |

8.2. Justificativa para os quantitativos estimados

8.2.1. A estimativa para a presente contratação tem como base a demanda recorrente do COTEC de Sobral por soluções robustas de segurança da informação, aliada à constatação de que os recursos contratados anteriormente chegaram ao fim da sua vigência. Além disso, destaca-se que o objeto ora proposto contempla um escopo significativamente ampliado em relação ao contrato anterior, incluindo não apenas a aquisição da licença "SF SW/Virtual with Xstream Protection – 16 CORES & 24GB RAM – (Ativo/Passivo) pelo período de 5 (cinco) anos", mas também o serviço de instalação da solução em ambiente on-premise, garantindo uma implantação adequada às necessidades da autarquia.

Ressalta-se ainda que, enquanto o processo anterior previa cobertura por apenas 3 (três) anos, a nova solução contempla 5 (cinco) anos de vigência, ampliando o horizonte de proteção da rede institucional e reduzindo a necessidade de novas aquisições no curto e médio prazo. Essa ampliação temporal, aliada ao escopo mais completo, contribui para o valor superior da contratação atual, que, no entanto, representa um investimento mais estratégico e duradouro.

Ainda que o valor desta contratação seja superior ao do contrato anterior, o investimento se justifica plenamente diante dos avanços proporcionados pela nova solução:

- Segurança Reforçada;
- Gestão Centralizada;
- Melhor Desempenho;
- Atualizações e Suporte Contínuos;
- Alta Disponibilidade;
- Conformidade com Normas;
- Otimização do Controle de Acesso;

Dessa forma, a contratação ora proposta representa não apenas uma continuidade, mas uma evolução substancial da política de segurança da informação da autarquia, alinhada às melhores práticas do setor e à crescente criticidade das operações digitais institucionais.

8.2.3. Locais onde serão utilizados:

| LOCAIS ONDE SERÃO UTILIZADOS | VALOR A SER CONTRATADO |
|---|---|
| COORDENADORIA DE GESTÃO DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - SEPLAG | R$ 2.783.033,60 |

## 9. Estimativa do valor da contratação

9.1. As unidades de medida de cada item da contratação, a quantidade estimada dos serviços e o valor estimado na contratação baseou-se nos parâmetros estabelecidos no art. 23 da Lei 14.133/2021, bem como no art. 19 do Decreto Municipal nº 3.212/2023. As memórias de cálculo e documentos que lhe deram suporte, constam em anexo a este ETP, bem como as devidas justificativas.

9.2. Referência de preços:

| **VALOR A SER CONTRATADO: R$ 2.783.033,60 (dois milhões, setecentos e oitenta e três mil, trinta e três reais e sessenta centavos)** | | | | | | |
|---|---|---|---|---|---|---|
| **ITEM** | **ESPECIFICAÇÃO** | **UNIDADE DE MEDIDA** | **QTD** | **PROPONENTE** | **VALOR MENSAL** | **VALOR TOTAL (60 MESES)** |
| 1 | Serviços de proteção do tráfego de rede de próxima geração (on premise) do Tipo A. | UNIDADE | 1 | ARP 6/2025 - COFEN/DF | R$ 46.100,56 | R$ 2.766.033,60 |
| | | | | DAMSAFE SOLUÇÕES EM SISTEMAS EMPRESARIAIS LTDA | R$ 63.550,00 | R$ 3.813.000,00 |
| | | | | FULLPAR EMPREENDIMENTOS, TECNOLOGIA E PARTICIPAÇÕES LTDA | R$ 65.000,00 | R$ 3.900.000,00 |
| | | | | LIVETECH DA BAHIA INDUSTRIA E COMERCIO S. A | R$ 57.500,00 | R$ 3.450.000,00 |
| 4 | Instalação da solução de proteção do tráfego de rede de próxima geração (on premise) do Tipo A | UNIDADE | 1 | ARP 6/2025 - COFEN/DF | R$ 17.000,00 | R$ 17.000,00 |
| | | | | DAMSAFE SOLUÇÕES EM SISTEMAS EMPRESARIAIS LTDA | R$ 85.000,00 | R$ 85.000,00 |
| | | | | FULLPAR EMPREENDIMENTOS, TECNOLOGIA E PARTICIPAÇÕES LTDA | R$ 25.000,00 | R$ 25.000,00 |
| | | | | LIVETECH DA BAHIA INDUSTRIA E COMERCIO S.A | R$ 90.000,00 | R$ 90.000,00 |

9.3. O custo estimado total da contratação da empresa fornecedora da Ata de Registro de preços ora aderida importa na quantia de R$ 2.783.033,60 (dois milhões, setecentos e oitenta e três mil, trinta e três reais e sessenta centavos).

## 10. Descrição da solução como um todo considerando todo o ciclo de vida do objeto

A solução proposta contempla a implementação de um firewall de próxima geração (Next Generation Firewall – NGFW) voltado à proteção proativa e inteligente do tráfego de rede da instituição, abrangendo todo o ciclo de vida do objeto, desde a sua aquisição até a plena operação e manutenção ao longo de cinco anos. A estrutura da solução está ancorada na aquisição da licença **"SF SW/Virtual with Xstream Protection – 16 CORES & 24GB RAM (Ativo/Passivo)"**, com vigência de 60 meses, garantindo alta disponibilidade (HA) e resiliência operacional através do modelo ativo/passivo. A proteção Xstream assegura funcionalidades avançadas de inspeção profunda de pacotes (DPI), controle granular de aplicações, mitigação contra ameaças zero-day, inspeção SSL/TLS, além de recursos de

sandboxing e inteligência artificial aplicada à detecção de anomalias. O ciclo de vida do objeto inicia-se com o **fornecimento da licença e o serviço de instalação on-premise**, etapa em que será realizada a configuração inicial do ambiente virtualizado, o provisionamento de recursos, a integração à infraestrutura de rede existente e a validação das políticas de segurança. Esta etapa também contempla o planejamento da topologia lógica do firewall e a definição dos perfis de proteção, alinhados com as melhores práticas e com os requisitos técnicos e normativos da instituição. Durante os cinco anos de vigência, a solução contará com **atualizações contínuas de firmware e assinaturas de segurança**, o que garante a sua capacidade de adaptação a novas ameaças e vulnerabilidades. Esse processo contínuo de atualização é fundamental para assegurar que a solução mantenha sua eficácia ao longo do tempo, mantendo-se compatível com os padrões tecnológicos e os níveis de risco emergentes. Além disso, a arquitetura da solução permite **escalabilidade horizontal e vertical**, possibilitando a expansão conforme o crescimento das demandas institucionais, seja em capacidade de processamento, número de usuários ou volume de tráfego. Ao final do período contratado, a solução terá proporcionado uma **postura de segurança robusta, centralizada e de fácil gerenciamento**, com relatórios e logs detalhados que apoiam a auditoria, conformidade e a tomada de decisões estratégicas. A adoção de um firewall de próxima geração assegura uma gestão eficaz do risco cibernético, além de contribuir para a continuidade dos serviços críticos da instituição, com total aderência à Lei Geral de Proteção de Dados (LGPD) e demais regulamentações aplicáveis.

São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados. Os termos “possui”, “permite”, “suporta” e “é” implicam fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções.

O termo “e” implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções. Todos os equipamentos, produtos, peças ou softwares necessários à prestação dos serviços deverão ser novos e de primeiro uso, em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Já os softwares comerciais deverão, ainda, ser instalados em sua versão mais atualizada e estarem cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante. Todos os equipamentos e softwares fornecidos para a prestação dos serviços deverão ser fornecidos com as Licenças durante toda a vigência do contrato. O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou software utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia ou na exposição de avos a riscos de segurança.

**ITENS 01 – SERVIÇOS DE PROTEÇÃO DO TRÁFEGO DE REDE DE PRÓXIMA GERAÇÃO (ON PREMISE)** com as portas, conexões e cabeamentos disponibilizados pela Contratada, inclusive as SFP e SFP+ com as respectivas gbics).

CAPACIDADE E QUANTIDADES MÍNIMAS – Tipo A. A plataforma de segurança deve possuir no mínimo a capacidade e as características abaixo, por equipamento:

a) Performance mínima de 12 Gbps de throughput de IPS;

b) Performance mínima de 6.5 Gbps de throughput para Prevenção de Ameaças;

c) Performance mínima de 10 Gbps de throughput de NGFW;

d) Suporte a, no mínimo, 7.000.000 de conexões simultâneas;

e) Suporte a, no mínimo, 250.000 novas conexões por segundo;

f) Possuir o número irrestrito quanto ao máximo de usuários licenciados;

g) Possuir no mínimo 2 (duas) interfaces 10GbE SFP+ e 2 (duas) interfaces 1GE UTP;

h) Possuir 1 (uma) interface do po console ou similar;

i) Possuir 2 (duas) fonte 100-240VAC sendo pelo menos 1 opção hot-swap;

**CARACTERÍSTICAS GERAIS PARA FIREWALL DE PRÓXIMA GERAÇÃO**

Por terem a finalidade de proteger o ambiente tecnológico do Contratante que está exposto em toda rede mundial de computadores; por ser mais um item de averiguação técnica das soluções, certificando que passaram pelo crivo de organização especializada; e por não inviabilizar o certame, pelo rol de fabricantes que possuem tais certificações, deverão apresentar ao menos uma das seguintes certificações ou outra equivalente: ICSA labs, NSS labs, Common Criteria.

A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generaon Firewall (NGFW) e console de gerência, monitoração e logs.

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

As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

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

O software deverá ser fornecido em sua versão mais atualizada.

Deve possuir modo HA (modo de alta disponibilidade) e deve ser implementado no mínimo avo-passivo.

O HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo avo-passivo ou modo avo-avo e deve possibilitar monitoração de falha de link.

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

A atualização de software deverá enviar avisos de atualização automáticos.

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

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

As notificações deverão ser realizadas via email e SNMP.

Suportar SNMPv3 e Nelow.

O firewall deverá ser stateful, com inspeção profunda de pacotes.

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

As políticas de NAT deverão ser customizáveis para cada regra.

A proteção contra flood deverá ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS).

Proteção contra an-spoofing.

Suportar IPv4 e IPv6.

O IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.

Deve ter Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP).

Deve possuir tecnologia de conectividade SD-WAN.

Deve implementar balanceamento entre os links WAN com método SpillOver.

Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SDWAN.

Deve suportar o uso de, no mínimo, 3 (três) links.

Deve suportar o uso de links de interfaces físicas, subinterfaces lógicas de VLAN e túneis IPSec.

Deve gerar log de eventos que registrem alterações no estado dos links do SD-WAN, monitorados pela checagem de saúde.

A solução deverá ser capaz de medir o status de saúde do link baseando-se em critérios mínimos de: Latência, Jier 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.

A solução de SD-WAN deve ser capaz de apresentar de forma gráfica todos os dados de análise da saúde dos links, contendo gráficos que apresentam no mínimo os critérios descritos acima.

Os gráficos devem ser apresentados em tempo real e possibilitar a visualização histórica de pelo menos 24 horas, 48 horas, 1 semana e 1 mês.

A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP para avaliação mais precisa de links que possuem QoE configurado.

A solução deve possuir funcionalidade de criação da malha SD-WAN em diversos firewalls em um único concentrador.

Esta funcionalidade deve facilitar a configuração do SD-WAN de múltiplos firewalls, criando automaticamente todas as informações necessárias para que o SD-WAN aconteça, como pelo menos, mas não se limitando a: criação de rotas, regras de firewall, objetos e túneis VPNs necessárias.

A mesma console do concentrador de SD-WAN deve monitorar os links de cada dispositivo implementado, gerando uma visualização única de todos os dispositivos implementados.

Deve possibilitar o roteamento baseado em VPNs.

Deve suportar criar políticas de roteamento.

Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições:

a) Interface de entrada do pacote;

b) IPs de origem;

c) IPs de desno;

d) Portas de destino;

e) Usuários ou grupos de usuários;

f) Aplicação em camada 7;

I - Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento.

II - Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.

III - Deve suportar Extended VLAN.

IV - O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso.

V - A solução deverá permir port-aggregaon de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces.

VI - Deve permitir a configuração de jumbo frames nas interfaces de rede.

VII - Deve permitir a criação de um grupo de portas layer2.

VIII - A Solução física deverá apresentar compatibilidade com modens USB (3G/4G), onde apenas seja acionado na eventualidade de falha no link principal.

IX - A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP; O traffic shapping (QoS) deverá ser baseado em rede ou usuário.

X - A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.

XI - Deve possuir otimização em tempo real de voz sobre IP.

XII - Deve implementar o protocolo de negociação Link Aggregaon Control Protocol (LACP).

**CONTROLE POR POLÍTICAS DE FIREWALL**

Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.

O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.

As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.

Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

Controle de políticas por países via localização por IP.

Suporte a objetos e regras IPV6.

Suporte a objetos e regras multicast.

**PREVENÇÃO DE AMEAÇAS**

Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, Anti-Malware e Firewall de Proteção Web (WAF) integrados no próprio appliance de Firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).

As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.

Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras.

Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa.

A solução contratada deve realizar a emulação de malwares desconhecidos em ambientes de sandbox em nuvem.

Para a eficácia da análise de malwares Zero-Days, a solução de Sandobox deve possuir algoritmos de inteligência artificial, como algoritmos baseados em machine learning.

A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de anti-malware e, ao fim da análise do artefato, deverá gerar um relatório contendo o resultado da análise, bem como os screenshots das telas dos sistemas emulados pela plataforma.

Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em nuvem.

A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-emails.

A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript.

Deve ter proteção em tempo real contra novas ameaças criadas.

Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente.

Deve permitir o bloqueio de vulnerabilidades.

Deve permitir o bloqueio de exploits conhecidos.

Deve detectar e bloquear o tráfego de rede que busque acesso a command and control e servidores de controle utilizando múltiplas camadas de DNS, AFC e firewall.

Deve incluir proteção contra ataques de negação de serviços.

Ser imune e capaz de impedir ataques básicos como: SYN flood, ICMP flood, UDP Flood, etc.

Suportar bloqueio de arquivos por tipo.

Registrar na console de monitoração as seguintes informações sobre ameaças idenficadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

Os eventos devem identificar o país de onde partiu a ameaça.

Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por

usuários, grupos de usuários, origem, destino, zonas de segurança. O apliance deve ter a capacidade de atuar como um gateway antispam de modo que possa realizar filtragens dos emails e aplicar políticas.

O gateway de email incluso no apliance deve ter pelo menos as seguintes proteções:

a) Sender Policy Framework (SPF);

b) Domain Keys Idenfied Mail (DKIM);

c) Domain-based Message Authencation, Reporting & Conformance (DMARC);

d) Bounce Address Tag Validation (BATV).

O filtro de email deve quarentenar os emails suspeitos ou realmente maliciosos.

A solução deve possibilitar aos usuários acessarem um painel para verificação da sua caixa pessoal de quarentena, possibilitando então a liberação ou a exclusão das mensagens.

A função de antispam deve permitir a configuração de relays com a possibilidade de autenticação desses relays. A função de antispam deve possibilitar também o envio de emails seguros, realizando a criptografia das mensagens bem como dos seus anexos.

A função de antispam deve conter funcionalidades de prevenção a perda de dados (DLP) para evitar que informações sigilosas sejam vazadas.

O firewall de aplicação Web (WAF) deverá ter a função de reverse proxy, com a função de URL hardening realizando deep-linking e prevenção dos ataques de pathtraversal ou directory traversal.

O firewall de aplicação Web (WAF) deverá realizar cookie signing com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor.

O firewall de aplicação Web (WAF) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de performance do WAF e permissão e bloqueio de ranges de IP.

Deverá permitir a identificação dos IPs de origem através de proxy via “X-forward headers”.

Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a proteção da aplicação Web, podendo ser configuradas isoladamente ou simultaneamente.

Proteção pelo menos contra os seguintes ataques, mas não limitada a: SQL injection e Cross-site scripting.

**CONTROLE E PROTEÇÃO DE APLICAÇÕES**

Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado.

Deve ser possível inspecionar os pacotes criptografados com os algoritmos TLS 1.2 e TLS 1.3.

O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algoritmos: curvas elípticas (ECDH, ECDHE, ECDSA), DH, DHE, Authencation, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384.

O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não descriptografar, negar o pacote e criptografar para determinadas conexões criptografadas.

Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-topeer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web email e update de softwares.

Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP, Protocol, Dropbox Download, Easy Proxy, Facebook Graph API,Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.

Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenng, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Aachment, Posng, Quesons, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Applicaon, Aachment), Google Drive (Base, File Download, File Upload), Google Earth Applicaon, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive, File Upload e Download, Twier (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Aach) e Youtube (Video Search, Video Streaming, Upload, Website).

Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

Atualizar a base de assinaturas de aplicações automaticamente.

Reconhecer aplicações em IPv6.

Limitar a banda usada por aplicações (traffic shaping).

Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory e Azure AD, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

**CONTROLE E PROTEÇÃO WEB**

Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.

Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.

Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Acve Directory, Azure AD, Radius, E-directory e base de dados local.

Deve permitir autenticação em 2 fatores em conjunto com a autenticação Radius.

Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.

Possuir pelo menos 90 categorias de URLs.

Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

Deve ser capaz de forçar o uso da opção Safe Search em sites de busca.

Deve ser capaz de forçar as restrições do Youtube.

Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário.

Suportar a criação categorias de URLs customizadas.

Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada.

Suportar a inclusão nos logs do produto de informações das atividades dos usuários.

Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.

Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem.

Deve realizar caching do conteúdo web.

Deve realizar filtragem por mime-type, extensão e tipos de conteúdos avos, tais como, mas não limitado a: ActiveX, applets e cookies.

Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré-determinados para acessar sites na internet.

A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador.

Deve possuir capacidade de alguns usuários previamente selecionados realizarem um bypass temporário na política de bloqueio atual.

A solução deve permitir o enforce dos domínios do Google e Office365 afim de determinar em quais domínios os usuários poderão se autenticar.

**IDENTIFICAÇÃO DE USUÁRIOS**

Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ e via base de dados local para identificação de usuários e grupos, permitido granularidade de controle/políticas baseadas em usuários e grupos de usuários.

Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

Deve permitir autenticação em modos: transparente, autenticação proxy (explicito, NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64. Ao se utilizar da opção de proxy explicito, deve permitir a autenticação por cada conexão, a fim de garantir que usuários logados em servidores de multissessão sejam identificados corretamente pelo firewall, mesmo quando utilizando-se apenas 1 IP de origem;

Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory, Azure AD e eDirectory.

Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

**QUALIDADE DE SERVIÇO - QoS**

Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.

A solução deverá suportar Traffic Shaping (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado.

Suportar priorização Real-Time de protocolos de voz (VoIP).

Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP.

**REDES VIRTUAIS PRIVADAS - VPN**

Suportar VPN Site-to-Site e Cliente-to-Site.

Suportar IPsec VPN.

Suportar SSL VPN.

Suportar L2TP e PPTP.

Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.

Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL.

Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows e macOS.

Deve possuir opção de VPN IPSEC com client nativo do fabricante.

Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.

A VPN IPsec deve suportar: DES, 3DES, GCM, Suite-B, Autenticação MD5 e SHA-1;Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (Advanced Encrypon Standard); SHA 256, 384 e 512; Autenticação via cerficado PKI (X.509) e Pre-shared key (PSK).

Deve suportar nativamente a integração com a huawei, afim de estabelecer um túnel seguro entre os appliances e o VPN da huawei.

Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, An-Malware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

Suportar autenticação via AD/LDAP, Token e base de usuários local.

Permir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ e via base de dados local.

**GERÊNCIA ADMINISTRATIVA CENTRALIZADA**

Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.

O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

Estar licenciada para ser gerenciada pela console de gerenciamento do firewall.

Devem ser fornecidas soluções virtuais ou em nuvem ou via appliances desde que obedeçam a todos os requisitos desta especificação.

Deve ser centralizada a gerência de todas as políticas do firewall e configurações para estas soluções de firewall, sem necessidade de acesso direto aos equipamentos.

Deve permitir a criação de templates para configurações.

Deve possuir indicadores do estado de equipamentos e rede.

Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.

Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.

Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc).

Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll back de configurações para mudanças indesejadas.

Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.

Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.

Deve possibilitar o envio dos logs via syslog com conexão segura (TLS).

**GERÊNCIA DE LOGS E RELATÓRIOS CENTRALIZADOS**

Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.
Estar licenciada para gerenciar as soluções de firewall de próxima geração Tipo A.
Devem ser fornecidas soluções virtuais ou em nuvem ou via appliances desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 8TB de dados.
Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando. Deve possibilitar a identificação de ataques como a detecção de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.
Deve conter relatórios pré-configurados pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN.
Deve fornecer relatórios históricos para análises de mudanças e comportamentos.
Deve conter customizações dos relatórios para inserção de logotipos próprios.
Deve fornecer relatórios de compliance SOX, HIPAA e PCI.
Deve permitir a exportação via PDF ou Excel.
Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.
Deve fornecer relatórios de tendências.
Deve fornecer logs em tempo real, de auditoria e arquivados.
Deve possuir mecanismo de procura de logs arquivados.
Deve ter acesso baseado em Web com controles administrativos distintos.
A Contratada deverá fornecer tudo que se fizer necessário para que todas as características e funcionalidades descritas neste termo funcionem plenamente.

**ITEM 04 – IMPLANTAÇÃO DAS SOLUÇÕES INTEGRADAS DE SEGURANÇA**

A Contratada deverá oferecer implantação das soluções, com configuração, instalação, testes e fornecimento dos hardwares e softwares relacionados, em regime de comodato e de acordo com as regras e políticas exigidas pela equipe técnica do Contratante, dentro do escopo das funcionalidades de cada serviço.
Deverão ser apresentados os seguintes entregáveis durante a implantação:
Fase de desenho da arquitetura.
Esquema detalhado de conexão com dispositivos.
Fase de Instalação.

A Contratada confeccionará relatório(s) final(is) sobre as atividades realizadas e com recomendações ao Contratante. Este relatório poderá ser entregue em até 25 dias úteis após a realização dos trabalhos. No relatório entregue constarão as seguintes seções:

Introdução;

Análise do ambiente;

Atividades realizadas;

Configuração de políticas aplicadas;

Resultados obtidos (coberturas, eventos de segurança registrados);

Conclusões;

Recomendações Específicas;

Recomendações de Segurança Corporativa;

Todas as atividades envolvidas serão acompanhadas e coordenadas por técnicos do Contratante.

A implantação das soluções, quando realizada no ambiente de produção, poderá ter as atividades executadas após o expediente (horários noturnos ou em finais de semana e feriados).

A Contratada será responsável por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional do Contratante, sem prejuízo aos serviços desta.

Quando previamente acordado entre as partes, a Contratada poderá realizar serviços de monitoramento in loco com o acompanhamento de um representante da instituição.

A instalação dos equipamentos e sistemas que permitirão a prestação dos serviços de que trata este Estudo Técnico Preliminar deverá ser executada pela Contratada nos prédios do Contratante.

Deve abranger a instalação física e lógica da solução, em sua totalidade, com duração máxima de 7 (sete) dias corridos, compreendendo, mas não se limitando a essas, as seguintes atividades:

Instalação física ou virtual dos equipamentos nas dependências ou no ambiente tecnológico do Contratante.

Identificação de conformidade com os pré-requisitos da ferramenta, de acordo com as melhores práticas ditadas pelo fabricante, no sendo de melhorar o gerenciamento e performance e aplicar os “patchs” para atualização do sistema, quando necessário.

Definição das funcionalidades a serem implantadas.

Definição da parametrização.

Instalação e configuração de toda a solução com vista ao gerenciamento dos recursos solicitados neste ETP em sua totalidade.

A instalação deve contemplar a verificação da infraestrutura elétrica e lógica existente. Eventuais problemas e necessidade de ajustes devem ser comunicados ao Contratante o qual será responsável pela solução de tais problemas.

A instalação dos equipamentos e componentes da solução deverá levar em consideração o ambiente e instalações existentes (espaço físico, sistema de refrigeração e de fornecimento de energia elétrica, dutos, eletrocalhas, entre outros elementos). Os componentes fornecidos (equipamentos e acessórios) devem proporcionar condições ideais de funcionamento tanto no que diz respeito à disposição física nas salas e nos “rack’s” evitando problemas de refrigeração e de acesso físico.

Após a instalação dos equipamentos, alimentação elétrica e conexões com a rede de dados e/ou voz, não poderá haver cabos sem proteção, soltos, por cima do piso elevado ou que obstruam a frente ou visibilidade dos equipamentos instalados.

Os serviços de instalação e configuração deverão ser prestados nas dependências do Contratante.

**REQUISITOS GERAIS PARA A PRESTAÇÃO DOS SERVIÇOS**

É responsabilidade da Contratada quaisquer danos físicos aos equipamentos durante os processos de instalação e configuração.

É proibida a divulgação de quaisquer aspectos da configuração desses equipamentos, por questões de sigilo e segurança, por parte dos técnicos responsáveis pela instalação e configuração, ou quaisquer outros que tenham acesso a essas informações, salvo quando houver autorização por escrito do Contratante.

Todas as senhas criadas e os usuários cadastrados nos processos de instalação e configuração dos equipamentos devem ser registrados e entregues por escrito ao responsável técnico indicado pela SEPLAG.

Deverá ser entregue ao responsável técnico indicado pela SEPLAG relatório com todos os procedimentos e configurações executados, assinado pelo responsável técnico da Contratada.

O início dos serviços deve ocorrer obedecendo os prazos dispostos no termo de referência.

A Contratada deve executar, prioritariamente, como parte obrigatória do processo de instalação e sempre que aplicável a cada solução, as seguintes atividades:

a) Definição de políticas e regras de proteção do perímetro “internet” visando conformidade com as normas ISO/IEC 17799 e NBR-ISO/IEC 17799, que tratam de segurança da informação e das configurações abaixo;

b) Configuração da console de gerenciamento;

c) Migração das regras existentes na solução de segurança atual do Contratante;

d) Configuração da autenticação de usuários integrada ao domínio da rede "Microsoft", via ferramenta nativa de integração da solução;

e) Análise de falsos positivos que podem ser gerados após implantação;

f) Adequações pós-instalação;

g) Instalação e configuração dos "firewall's" em modo "cluster" avo/avo ou avo/passivo;

h) Instalação e configuração do concentrador de "logs", "archive" e relatórios;

i) Instalação e configuração dos "gateway's" "SMTP" em modo "cluster" avo/avo ou avo/passivo;

j) Migração, adequação e definição, juntamente com a equipe de Tecnologia da Informação do Contratante das políticas para controle de tráfego de entrada e saída de dados;

k) Execução de testes de segurança através da análise de vulnerabilidades completa do perímetro de internet;

l) Documentação de todas as configurações realizadas em todas as soluções implantadas;

m) Realização de testes, certificação e otimização de todas as soluções implantadas;

n) Entrega da documentação de todo o projeto.

## 11. Justificativa para o Parcelamento ou não da Solução

11.1. Não se aplica em exame da natureza do serviço que ora se pretende contratar nessa adesão.

## 12. Demonstrativo dos resultados pretendidos

12.1. A contratação de uma nova solução de firewall tem como objetivo fortalecer a segurança, a disponibilidade e a integridade da rede da Prefeitura, assegurando padrões elevados de proteção da informação. Espera-se, com isso, aprimorar de forma significativa o gerenciamento centralizado da infraestrutura de rede, proporcionando um serviço mais eficiente, estável e confiável para todos os usuários.

12.2. A seguir, detalham-se os resultados pretendidos com a contratação:

- Segurança Reforçada:
  Proteção avançada contra ataques cibernéticos, malwares e acessos não autorizados;
- Gestão Centralizadas:
  Facilidade na administração das regras de segurança e controle de acesso em um único ambiente.
- Melhor Desempenho:
  Capacidade de suportar o tráfego crescente sem comprometer a disponibilidade da rede;
- Atualizações e Suporte:

Garantia de suporte técnico e atualizações regulares do fabricante, reduzindo vulnerabilidades;

- Alta Disponibilidade:
  Redundância e continuidade dos serviços, evitando falhas e interrupções na conectividade;

- Conformidades com Normas:
  Atendimento a requisitos de segurança da informação e políticas institucionais;

- Otimização do Controle de Acesso:
  Gerenciamento eficiente do uso da internet e das aplicações dentro da rede.

**11. Providências a serem adotadas previamente a celebração do contrato**

11.1. Para garantir que a contratação seja realizada de forma eficiente, segura e dentro da legalidade, a Administração Pública deve adotar uma série de providências antes da celebração do contrato.

A seguir, estão as principais etapas e ações a serem realizadas:

1. Elaboração do Termo de Referência: Incluir uma descrição detalhada do serviço a ser contratado, com as especificações técnicas que se fizerem necessárias.

2. Análise Jurídica e Apreciação pela Assessoria Jurídica.

3. Conformidade Legal: Submeter a minuta do contrato à análise da Assessoria Jurídica para garantir que todos os aspectos legais estão contemplados e que o contrato está em conformidade com a legislação vigente.

4. Aprovação e Assinatura: Após a aprovação da Assessoria Jurídica.

5. Verificação da disponibilidade orçamentária e financeira para a contratação.

6. Comprovação de que a proponente preenche os requisitos de habilitação e qualificação técnica.

7. Razão da escolha da contratada, justificativa do preço e autorização da autoridade competente.

7. Convocação para assinatura do contrato.

8. Gestão e Fiscalização do Contrato: Designação de um Fiscal de Contrato: Nomear um servidor responsável por acompanhar a execução do contrato, garantindo que as entregas sejam feitas conforme acordado e que eventuais problemas sejam solucionados prontamente.

9. Monitoramento da Execução: Acompanhar a aquisição, implementação e funcionamento das rotinas de trabalhos, observando conforme estabelecido no Termo de Referência.

10. Gestão de Pagamentos: Efetuar os pagamentos conforme as etapas de execução do contrato, garantindo que todos os pagamentos sejam realizados apenas após a confirmação da entrega do insumo.

**12. Contratações Correlatas e/ou Interdependentes**

12.1. Para esta solução **não há** contratações correlatas nem interdependentes que guardam relação/afinidade/dependência com o objeto da compra/contratação pretendida, sejam elas já realizadas ou contratações futuras.

**14. Posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina**

14.1. A adesão à Ata de Registro de Preços Nº 6/2024, oriunda do Pregão Eletrônico Nº 90.028/2024, apresenta-se como a solução mais adequada e eficiente para suprir a necessidade da infraestrutura de segurança da rede institucional, por meio da aquisição de uma solução de firewall de próxima geração. A escolha dessa modalidade de contratação garante a obtenção da tecnologia de forma célere, segura e economicamente vantajosa, evitando a morosidade e os riscos inerentes à realização de um novo processo licitatório. Além disso, a contratação atende plenamente às exigências técnicas da área de TI, assegurando a implementação e o funcionamento contínuo de uma solução robusta de segurança cibernética, essencial para a proteção do tráfego de rede, a prevenção de ameaças avançadas e a garantia da integridade e disponibilidade dos sistemas críticos da instituição.

14.2. Com base nos elementos obtidos neste estudo técnico preliminar, declaramos que é VIÁVEL a presente contratação, sendo, portanto, a mais adequada para o atendimento da necessidade em questão.

Documento assinado digitalmente
ANA VALDELIA PINTO DE VASCONCELOS FARIAS
Data: 15/05/2025 16:29:31
Verifique em https://validar.iti.gov.br

**Ana Valdelia Pinto De Vasconcelos Farias**
Matrícula Nº03579
Presidente da Equipe de Planejamento

Documento assinado digitalmente
MARAIZA MARIA BATISTA SILVA
Data: 15/05/2025 16:32:39
Verifique em https://validar.iti.gov.br

**Maraiza Maria Batista Silva**
Matrícula Nº48621
Membro da Equipe de Planejamento

Documento assinado digitalmente
VIRNA LISSE VASCONCELOS CARNEIRO
Data: 15/05/2025 16:37:54
Verifique em https://validar.iti.gov.br

**Virna Lisse Vasconcelos Carneiro**
Matrícula Nº48954
Membro da Equipe de Planejamento

Aprovado:

Documento Assinado Digitalmente
ELVIS CORIOLANO DE SOUSA SILVA
Data: 15/05/2025 16:41

**Elvis Coriolano de Sousa Silva**
Coordenador Administrativo Financeiro