Av. Fiorentino Bacchi, nº 673 - Cep: 99840-000
Estado do Rio Grande do Sul/BR
Contato: (54) 99669-0941

ETP – ESTUDO TÉCNICO PRELIMINAR

Descrição da necessidade:	A presente contratação tem por objetivo a aquisição de uma solução de Firewall de Próxima Geração (Next-Generation Firewall – NGFW) para atender às necessidades da Prefeitura Municipal de Sananduva/RS. O avanço das tecnologias da informação e comunicação, aliado à crescente digitalização dos serviços públicos, impõe à Administração Pública o desafio de proteger sua infraestrutura de rede, servidores e estações de trabalho (endpoints) contra ameaças cibernéticas cada vez mais sofisticadas. A segurança da informação tornou-se condição indispensável para a continuidade dos serviços públicos, a proteção dos dados dos munícipes e a conformidade com a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018). A necessidade da contratação decorre da obrigatoriedade de garantir que a rede corporativa da Prefeitura opere em ambiente seguro, confiável e resiliente, com mecanismos avançados de defesa contra ataques como: intrusões, malware, ransomware, vazamento de informações, acessos não autorizados e outras ameaças emergentes no cenário digital. A solução deverá contemplar, no mínimo: - Proteção avançada contra ameaças (ATP), com inspeção profunda de pacotes e identificação de tráfego malicioso em tempo real; - Gerenciamento centralizado e intuitivo, permitindo administração unificada das políticas de segurança; - Controle de aplicações e usuários, com monitoramento detalhado de acessos e recursos utilizados; - Integração com soluções de antivírus, antimalware e sandboxing para detecção e mitigação de ameaças avançadas; - Recursos de alta disponibilidade (HA), assegurando a continuidade dos serviços em caso de falha de hardware ou software; - Escalabilidade para suportar o crescimento da demanda de tráfego de rede da Administração; - Desempenho adequado para não comprometer a experiência do usuário e a execução dos sistemas críticos. Assim, a contratação da solução de NGFW se mostra imprescindível para assegurar a proteção integral da infraestrutura de TI da Prefeitura de Sananduva/RS, garantindo a continuidade dos serviços públicos digitais, essenciais à população; A proteção de dados sensíveis dos munícipes e da própria Administração; A mitigação de riscos legais e operacionais relacionados à indisponibilidade de sistemas críticos; A modernização da gestão pública em conformidade com os princípios da eficiência, economicidade e segurança da informação.

		Portanto, a presente contratação atende a uma necessidade estratégica da Administração Municipal, alinhada às melhores práticas de governança e segurança da informação, sendo medida indispensável para a proteção dos ativos digitais e a manutenção da confiança da sociedade nos serviços prestados pelo Poder Público.
02	Lista de áreas requisitantes que solicitaram a contratação	Secretaria Municipal de Planejamento e Administração
03	Compatibilidade com o PAC (Plano Anual de Contratações)	No momento, o Município ainda não possui um Plano Anual de Contratações.
04	Requisitos da contratação	A empresa contratada deverá atender aos seguintes requisitos mínimos durante toda a vigência da contratação: - A contratação será realizada com empresa regularmente constituída, inscrita no Cadastro Nacional da Pessoa Jurídica (CNPJ); - A licitante deverá comprovar, na fase de habilitação, sua regularidade fiscal, trabalhista e econômico-financeira, mediante apresentação das seguintes documentações: Certidão conjunta da Receita Federal e Dívida Ativa da União; Certidão de Regularidade do FGTS (CRF); Certidão Negativa de Débitos Trabalhistas (CNDT); Certidões negativas de débitos estaduais e municipais, do domicílio ou sede da empresa; Certidão negativa de falência, recuperação judicial ou extrajudicial, nem em estado de concordata ou dissolução. - Especificações Técnicas Mínimas: **Capacidade de Processamento** - Capacidade de IPS (Intrusion Prevention System): 1,4 Gbps - Capacidade de NGFW: 1 Gbps - Capacidade de Proteção contra Ameaças: 800 Mbps **Desempenho do Sistema** - Capacidade de Firewall: 10 Gbps / 10 Gbps / 6 Gbps - Latência do Firewall: 2,54 µs (para pacotes UDP de 64 bytes) - Taxa de Processamento do Firewall: 9 Mpps (milhões de pacotes por segundo) - Sessões Concorrentes (TCP): 800.000 - Novas Sessões por Segundo (TCP): 35.000 - Número de Políticas de Firewall: 5000 **Segurança e Proteção** - VPN IPsec: Capacidade de Throughput: 6,1 Gbps (para pacotes de 512 bytes); Túneis Gateway-to-Gateway: 200; Túneis Client-to-Gateway: 500 - VPN SSL: Capacidade de Throughput: 405 Mbps; Usuários Concorrentes (Modo de Túnel): 200

		- Inspeção SSL/TLS: Throughput de Inspeção SSL (IPS, HTTPs): 405 Mbps; SSL Inspection Concurrent Session (IPS, avg. HTTPS): 100.000; CPS (Conexões por Segundo) de Inspeção SSL: 400 - Controle de Aplicações: Throughput de Controle de Aplicações: 1,8 Gbps - Throughput de CAPWAP (para APs): 8,5 Gbps **Interfaces de Hardware** - Portas GE RJ45 WAN/DMZ: 3 - Portas GE RJ45 Internas: 7 - Portas USB: 1 - Console (RJ45): 1 OBS: Todas as portas RJ45 deverá ser permitido a alteração de sua função (LAN, WAN, DMZ). **Recursos Adicionais** - Security Fabric: A solução deve ser capaz de integrar e orquestrar múltiplos produtos de segurança para fornecer uma visão unificada e proteção abrangente. - Networking: Deve suportar roteamento dinâmico, balanceamento de carga, e ter funcionalidades de VPN avançadas para garantir conectividade segura e eficiente. - Controlador Wireless: A solução deve incluir um controlador wireless integrado, permitindo o gerenciamento de pontos de acesso (APs) diretamente pelo firewall. - Alta Disponibilidade: Deve suportar configuração de alta disponibilidade (HA) com modos Active-Active, Active-Passive e Clustering, garantindo continuidade de serviço. - Gerenciamento: Interface de gerenciamento centralizada via web, com suporte a HTTPS, SSH e SNMP. Deve permitir gerenciamento local e remoto, além de integrar com soluções SIEM para monitoramento de eventos. - Scripting: Suporte a scripts para automação de tarefas de configuração e operação, permitindo maior flexibilidade e eficiência no gerenciamento da segurança. - Certificação: O equipamento deve ser certificado por normas reconhecidas como ISO 27001, PCI-DSS e outras relevantes para o ambiente de segurança. - Logs: Deverá ser mantido os logs do Firewall, por um período mínimo de 1 ano. - Centro de Inteligência: A solução deve receber atualizações e assinaturas de segurança geradas por um centro de inteligência do próprio fabricante, garantindo a proteção contra as ameaças mais recentes. Essas atualizações devem ser automáticas e regulares, garantindo que o

equipamento esteja sempre atualizado com as últimas defesas contra vulnerabilidades conhecidas e ameaças emergentes.

- Armazenamento de Tráfego: A solução deve ser capaz de armazenar todo o tráfego de rede (não apenas o tráfego UTM) por um período mínimo de 365 dias. O armazenamento pode ser realizado na memória interna do appliance (não sendo permitido o uso de adaptadores, HD externo, pendrive, etc.) ou em uma plataforma cloud desenvolvida pelo próprio fabricante.
- Integração com Active Directory: O equipamento deve ser capaz de integrar com o Active Directory para autenticação dos usuários, suportando tanto autenticação passiva (SSO) quanto ativa, através de um portal cativo (captive portal).

Alta Disponibilidade e Resiliência

- Suporte a alta disponibilidade (HA) com failover automático.
- Suporte a balanceamento de carga.
- Configurações de alta disponibilidade: Active-Active, Active-Passive, Clustering.
- Domínios Virtuais: 10 / 10 (padrão / máximo).
- Número Máximo de Switches Suportados: 24.
- Número Máximo de APs Suportados: 64 / 32 (modo total / modo túnel).
- Número Máximo de Tokens Suportados: 500.

Atualizações e Suporte

- Suporte a atualizações automáticas de firmware e assinaturas de segurança.
- Contrato de suporte técnico 24/7 com tempo de resposta definido (SLA).
- Documentação completa em português para configuração e operação.
- RMA: A garantia deve cobrir a troca imediata do equipamento em um período máximo de 2 horas após constatada a necessidade do RMA.
- Suporte Presencial: Caso seja necessário atendimento presencial (in-loco), a contratada deverá atender a demanda no prazo máximo de 40 Minutos, a fim de evitar eventuais "downtime" e prejuízos ao atendimento à população.

Certificações e Conformidades

- Certificação ISO 27001 ou equivalente.
- Conformidade com as principais normas de segurança (como PCI-DSS, GDPR).

Entrega do Appliance e Licença

- Appliance Hardware e Licença: O fornecedor deve fornecer tanto o appliance hardware quanto a licença correspondente durante todo o período do contrato. A solução deve incluir todas as licenças necessárias para o funcionamento completo do firewall, incluindo atualizações e suporte técnico, de acordo com as especificações e requisitos descritos anteriormente.

<table>
<tr>
<td></td>
<td></td>
<td colspan="6">

Requisitos Adicionais

- O fornecedor deve realizar a instalação, configuração e teste do equipamento na sede da Prefeitura no máximo em 24 horas após a assinatura do contrato, e prestar todo o suporte técnico de forma presencial, com tempo máximo de 40 (quarenta) minutos para atendimento presencial.

- Treinamento para a equipe técnica da Prefeitura sobre as funcionalidades e administração da solução.

- Garantia mínima de 12 meses com possibilidade de extensão.

- Suporte às Demandas de Configuração: A contratada deverá atender todas as demandas de configuração relacionadas ao equipamento solicitadas pelo profissional de TI da Prefeitura.

Forma de Pagamento:

O pagamento será efetuado até o quinto dia útil do mês subsequente ao da prestação dos serviços, mediante a apresentação da nota fiscal correspondente, devidamente atestada pela Secretaria Municipal de Planejamento e Administração, comprovando a execução dos serviços conforme estabelecido no contrato. O pagamento estará condicionado à regularidade fiscal da contratada no momento da liquidação da despesa.

OBS: Além dos documentos listados acima, a licitante deverá apresentar todas as declarações, formulários e demais documentos que vierem a ser exigidos no Termo de Referência, sendo de sua inteira responsabilidade atentar-se ao cumprimento integral das condições estabelecidas no processo licitatório.

</td>
</tr>
<tr>
<td>05</td>
<td>Quantidade estimada da contratação</td>
<td colspan="6">
<table>
<tr><th>Item</th><th>DESCRIÇÃO</th><th>QTDE.</th><th>Unidade</th><th>Valor Máximo Mensal R$</th><th>Valor Máximo Total R$</th></tr>
<tr><td>01</td><td>Contratação de uma solução de Firewall de próxima geração (Next-Generation Firewall - NGFW), visa proteger a rede corporativa bem como os endpoint e servidores da Prefeitura municipal de Sananduva/RS. As soluções devem proporcionar segurança, desempenho e escalabilidade adequados às necessidades da administração pública, com foco em proteção contra uma ampla gama de ameaças avançadas bem como o gerenciamento centralizado e alta disponibilidade.</td><td>12</td><td>Meses</td><td>R$ 3.156,33 por mês.</td><td>R$ 37.875,99 por ano.</td></tr>
</table>
</td>
</tr>
</table>

06	Levantamento de mercado	O presente levantamento de mercado tem por finalidade identificar as alternativas existentes e justificar técnica e economicamente a contratação de uma solução de Firewall de Próxima Geração (Next-Generation Firewall – NGFW) destinada a proteger a rede corporativa, os endpoints e os servidores da Prefeitura Municipal de Sananduva/RS. Foram analisadas as modalidades de soluções ofertadas atualmente no mercado: **Appliances físicos dedicados** Solução baseada em equipamentos próprios para segurança de rede, com recursos de inspeção profunda de pacotes (DPI), prevenção de intrusões (IPS), inspeção de tráfego criptografado (TLS 1.3), controle de aplicações, VPN, alta disponibilidade (HA) e integração com serviços em nuvem. Vantagens: alto desempenho, confiabilidade e previsibilidade operacional. Desvantagens: maior investimento inicial (CAPEX). **Soluções virtuais (firewalls em máquinas virtuais)** Executadas em ambiente de virtualização ou em nuvem, com recursos similares às soluções físicas, mas dependendo de infraestrutura existente. Vantagens: flexibilidade de escalabilidade, menor custo inicial de hardware. Desvantagens: desempenho limitado aos recursos disponíveis na infraestrutura virtual; riscos de compartilhamento de recursos críticos. **Soluções híbridas (appliance + serviços em nuvem)** **Integram hardware local com funcionalidades adicionais em nuvem (ex.: sandbox, SD-WAN, CASB).** Vantagens: proteção ampliada para usuários remotos e melhor integração com ambientes modernos. Desvantagens: custos recorrentes de serviços e dependência de conectividade estável. Foram identificados como principais fornecedores com presença consolidada no Brasil: Fortinet, Palo Alto Networks, Check Point, Cisco, Sophos, SonicWall e WatchGuard, garantindo competitividade e diversidade de opções. **Justificativa técnica da escolha do tipo de solução** Considerando a criticidade dos serviços públicos municipais e a necessidade de garantir segurança, disponibilidade e desempenho, a solução que melhor atende às necessidades é a contratação de appliances físicos em arquitetura de alta disponibilidade (HA), complementados por serviços de segurança em nuvem quando aplicável. Essa escolha se justifica pelos seguintes aspectos: - Maior desempenho e confiabilidade, indispensáveis ao funcionamento contínuo da rede corporativa municipal;

<table>
<tr>
<td></td>
<td></td>
<td>- Alta disponibilidade, assegurando a continuidade de serviços essenciais mesmo em caso de falhas;
- Gerenciamento centralizado, permitindo controle, auditoria e padronização de políticas de segurança;
- Escalabilidade, possibilitando expansão de recursos sem substituição integral da infraestrutura;
- Suporte técnico especializado, com garantia de atualizações de segurança contínuas.
- Pesquisa de preços realizada em fornecedores locais e no Licitacon evidenciando o preço médio supracitado.
Diante das alternativas avaliadas, conclui-se que a solução mais compatível com as necessidades da Prefeitura é a contratação de uma solução de Firewall de Próxima Geração (Next-Generation Firewall – NGFW) destinada a proteger a rede corporativa, os endpoints e os servidores da Prefeitura Municipal.
A medida atende aos princípios da eficiência, economicidade e competitividade, previstos na Lei nº 14.133/2021, assegurando que a Administração obtenha o melhor custo-benefício com ampla participação de fornecedores no certame.</td>
</tr>
<tr>
<td>07</td>
<td>Estimativa de valor (baseado na cotação de preços a ser realizada – média, mediana ou menor valor)</td>
<td>
<table>
<tr><th>Item</th><th>Descrição</th><th>Fornecedor 01</th><th>Fornecedor 02</th><th>Fornecedor 03</th><th>Valor de Referência (média das 03 pesquisas)</th></tr>
<tr><td>01</td><td>Contratação de uma solução de Firewall de próxima geração (Next-Generation Firewall - NGFW), visa proteger a rede corporativa bem como os endpoint e servidores da Prefeitura municipal de Sananduva/RS. As soluções devem proporcionar segurança, desempenho e escalabilidade adequados às necessidades da administração pública, com foco em proteção contra uma ampla gama de ameaças avançadas bem como o</td><td>R$
3.979,00</td><td>R$
3.000,00</td><td>R$
2.490,00</td><td>R$
3.156,33</td></tr>
</table>
</td>
</tr>
</table>

			gerenciamento centralizado e alta disponibilidade.				
08	Descrição da solução	A solução a ser contratada consiste no fornecimento, implantação, configuração e suporte de uma plataforma de segurança de rede do tipo Firewall de Próxima Geração (Next-Generation Firewall – NGFW), destinada a proteger a infraestrutura tecnológica da Prefeitura Municipal de Sananduva/RS, abrangendo servidores, endpoints e a rede corporativa como um todo. A solução deverá contemplar os seguintes aspectos: **Funcionalidades principais** - Inspeção profunda de pacotes (DPI) com capacidade de identificar e controlar aplicações independentemente de portas ou protocolos; - Sistema de prevenção de intrusões (IPS/IDS) atualizado em tempo real; - Filtragem de conteúdo web e controle de aplicações com base em políticas de segurança definidas pela Administração; - Inspeção de tráfego criptografado (TLS 1.3) sem degradação significativa de desempenho; - Serviços de segurança avançada, incluindo antimalware, prevenção contra ameaças de dia zero, proteção contra ransomware, sandboxing e reputação de endereços IP/domínios; - Suporte a VPNs seguras (IPSec e SSL), para usuários remotos e comunicação entre unidades administrativas; - Recursos de SD-WAN, para otimização e priorização de tráfego entre unidades interligadas; - Alta disponibilidade (HA) em arquitetura redundante (ativo-passivo ou ativo-ativo), assegurando a continuidade dos serviços em caso de falha; - Gerenciamento centralizado, permitindo a aplicação uniforme de políticas de segurança e integração com sistemas de monitoramento e auditoria já existentes. **Requisitos de desempenho mínimos** - Throughput de firewall e IPS compatíveis com o porte da rede municipal; - Número de sessões simultâneas e túneis VPN dimensionados de acordo com a demanda estimada; - Latência mínima e suporte a enlaces de Internet de alta capacidade. **Manutenção e assistência técnica** A contratada deverá assegurar: - Suporte técnico especializado em língua portuguesa, com atendimento remoto e, quando necessário, presencial, durante todo o período contratual; - Tempo máximo de resposta para abertura de chamados e de solução de incidentes, compatível com a criticidade do serviço (SLA); - Atualizações contínuas de firmware e assinaturas de segurança, garantindo a proteção contra novas ameaças cibernéticas;				

		- Manutenção preventiva e corretiva, com substituição de hardware em caso de falha, sem ônus adicional à Administração; - Equipe certificada pelo fabricante para instalação, configuração e suporte da solução; - Documentação técnica completa e manual de operação para a equipe de TI da Prefeitura; - Treinamento inicial para os técnicos municipais responsáveis pela gestão da solução. **Prazo e garantia** - A solução deverá ser entregue em condições plenas de funcionamento, devidamente configurada e testada; - O contrato deverá incluir garantia de fábrica e suporte de segurança por, no mínimo, 36 (trinta e seis) meses, contemplando hardware, software, atualizações e serviços de assistência técnica.
09	Parcelamento da contratação	Não se aplica.
10	Resultados esperados e providências a serem tomadas caso haja intercorrências	Com a implantação da solução de Firewall de Próxima Geração (NGFW), espera-se: - Aprimoramento da segurança da informação, com proteção efetiva da rede corporativa, servidores e endpoints contra ameaças avançadas (malwares, ransomware, intrusões e ataques de negação de serviço). - Continuidade dos serviços públicos municipais, assegurada pela arquitetura de alta disponibilidade (HA), evitando interrupções críticas decorrentes de falhas de hardware ou software. - Centralização e padronização da gestão de segurança, por meio de console único de administração, facilitando auditoria, aplicação de políticas e resposta a incidentes. - Redução de vulnerabilidades e riscos cibernéticos, mediante inspeção de tráfego criptografado, controle de aplicacões e atualizações constantes de assinaturas de segurança. - Eficiência operacional, com menor esforço da equipe de TI para manter e monitorar a infraestrutura de segurança, liberando recursos humanos para outras demandas estratégicas. - Previsibilidade orçamentária, com contratos que incluam licenciamento, suporte e atualizações pelo período mínimo de 36 meses, evitando custos adicionais não previstos. **Providências em Caso de Intercorrências** Caso ocorram falhas, indisponibilidades ou não conformidades na execução do contrato, deverão ser adotadas as seguintes providências: - Abertura imediata de chamado junto ao suporte da contratada, com registro do protocolo e prazo estimado para resolução.

Av. Fiorentino Bacchi, nº 673 - Cep: 99840-000
Estado do Rio Grande do Sul/BR
Contato: (54) 99669-0941

		- Acionamento do SLA (Service Level Agreement) previstc contratualmente, garantindo prazos de atendimento e solução compatíveis com a criticidade dos serviços públicos. - Substituição temporária ou definitiva do equipamento, sem ônus para a Administração, em caso de falhas de hardware que não possam ser resolvidas em prazo aceitável. - Comunicação formal à Administração, por parte da contratada, sobre a natureza da intercorrência, medidas adotadas e previsão de restabelecimento do serviço. - Aplicação de penalidades contratuais, nos termos da Lei nº 14.133/2021 e do edital, caso haja descumprimento reiterado dos níveis de serviço acordados. - Plano de contingência: nos casos de incidentes de segurança críticos, a contratada deverá atuar em conjunto com a equipe de TI da Prefeitura para mitigação imediata do problema, priorizando a continuidade dos serviços essenciais.
11	Contratações correlatas a serem realizadas para complementação da contratação (Ex; materiais a serem adquiridos, cursos especializados, etc...)	No momento, não foi identificado a necessidade de contratação correlatada para a instalação dos objetos.
12	Impactos ambientais gerados pela contratação	Não há.
13	Análise de Risco da Contratação	Nos termos do art. 18, inciso VII, da Lei Federal nº 14.133/2021, a Administração deve avaliar e registrar os riscos que possam comprometer o êxito da contratação. Para o objeto em análise — aquisição de solução integrada de Firewall de Próxima Geração (NGFW) — foram identificados os seguintes riscos potenciais e respectivas medidas de mitigação: **Riscos Técnicos** - Equipamento fornecido não atender às especificações mínimas (throughput, SSL, VPN, HA) Mitigação: exigir laudos de conformidade do fabricante, homologação e realização de teste de aceite na instalação. - Incompatibilidade da solução com a infraestrutura de rede existente. Mitigação: vistoria técnica prévia e participação da equipe de TI da Prefeitura na fase de instalação. - Ausência de atualização de firmware e falhas no suporte técnico. Mitigação: prever em contrato suporte contínuo com SLA definido, além de comprovação de que o fornecedor é parceiro oficial do fabricante. **Riscos Operacionais** - Atrasos na entrega e instalação do equipamento.

		Mitigação: fixação de cronograma detalhado, aplicação de penalidades contratuais e acompanhamento pela fiscalização. - Falta de capacitação dos servidores municipais para operar a solução. Mitigação: incluir no contrato treinamento prático e teórico com emissão de certificado para a equipe de TI da Prefeitura. **Riscos Jurídico-Administrativos** - Exigências técnicas excessivamente restritivas que limitem a competitividade. Mitigação: permitir certificações equivalentes e justificar tecnicamente requisitos específicos no edital. - Impugnações ou recursos administrativos durante o pregão presencial. Mitigação: elaboração de edital claro, análise jurídica prévia e respostas tempestivas aos questionamentos. **Riscos Financeiros** - Sobrepreço ou superfaturamento. Mitigação: elaboração de orçamento de referência com base em ampla pesquisa de mercado. - Atrasos em repasses ou empenho. Mitigação: certificação prévia da disponibilidade orçamentária e previsão de fluxo financeiro compatível com a execução. **Riscos Ambientais** - Geração de resíduos eletrônicos ao final da vida útil do equipamento. Mitigação: exigir destinação ambientalmente adequada conforme a Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010). - Consumo elevado de energia elétrica. Mitigação: priorizar equipamentos certificados em eficiência energética (Energy Star ou equivalentes). A análise demonstra que os riscos identificados são mínimos e controláveis, desde que observadas as medidas de mitigação descritas. Com o adequado planejamento, fiscalização e cumprimento das normas técnicas, conclui-se que a contratação é plenamente viável e segura, garantindo a proteção da infraestrutura de rede e a continuidade dos serviços públicos digitais do Município de Sananduva.
14	Conclusão do ETP (viabilidade da contratação – é possível a contração?)	A Contratação atende ao interesse público e é perfeitamente viável.

Sananduva, 10 de setembro de 2025.

Av. Fiorentino Bacchi, nº 673 - Cep: 99840-000
Estado do Rio Grande do Sul/BR
Contato: (54) 99669-0941

Aline da Silva Ficagna

Aline da Silva Ficagna
Agente de contratação suplente conforme Portaria nº 097/2025

Sérgio Luiz Fracasso
Secretário de Planejamento e Administração

SANANDUVA
GOVERNO MUNICIPAL

Av. Fiorentino Bacchi, nº 673 - Cep: 99840-000
Estado do Rio Grande do Sul/BR
Contato: (54) 99669-0941

Material:

( ) Consumo
( ) Permanente
(X) Serviços

Fonte de Recursos:

Recursos Próprios do Município.

SOLICITAÇÃO DE ABERTURA DE PROCESSO LICITATÓRIO FORMALIZAÇÃO DE DEMANDA

Setor Solicitante (Secretaria(s) Competente(s)): Secretaria de Planejamento e Administração

Justificativa	Responsável
A Contratação de solução de Firewall, conforme especificada neste edital permitirá aumentar os atuais níveis de segurança e proteção das informações, notoriamente, indispensável para o desenvolvimento dos trabalhos nas repartições públicas, assim como aprimorará os níveis de segurança cibernética e proteção de dados, sendo essas soluções de segurança e proteção de dados extremamente importantes para proteger os dados, informação e sistemas do município contra acessos indevidos, ataques cibernéticos e vazamento de dados. A segurança da infraestrutura de TI é crucial para proteger os dados, sistemas e ativos da organização. Também se torna vital que tais sistemas sejam adequadamente instalados, configurados e com constante manutenção. A contratação de serviços de segurança visa mitigar riscos como ataques cibernéticos, vazamento de informações confidenciais, e interrupções no funcionamento dos sistemas. Investir em segurança é uma medida preventiva para evitar prejuízos financeiros, danos à reputação da Prefeitura, e prove um melhor atendimento ao público. Considerando as demandas atuais em segurança, principalmente após a Lei Geral de Proteção de Dados (Lei 13.709/2018), seria imprudente se o município não tomasse precauções a respeito, além de eventuais atos de crimes o que agregará ganhos e melhorias importantes para realização dos trabalhos dos órgãos do município de Sananduva/RS e seus usuários.	Existe a necessidade de aquisição material / serviço descrito abaixo. Estou de acordo com a solicitação e justificativa. Sérgio Luiz Fracasso Secretário de Planejamento e Administração Data: 10/09/2025

Indicação do responsável para fiscalização do contrato: Sérgio Luiz Fracasso

<u>Modalidade de licitação a ser utilizada:</u>

Av. Fiorentino Bacchi, nº 673 - Cep: 99840-000
Estado do Rio Grande do Sul/BR
Contato: (54) 99669-0941

( ) Chamamento Público

( ) Chamamento Público para Credenciamento

( ) Concorrência Pública Eletrônica

( ) Concorrência Pública Presencial - Encaminhar documento com justificativa conforme procedimento já adotado

( ) Pregão Eletrônico

(X) Pregão Presencial – Encaminhar documento com justificativa conforme procedimento já adotado

( ) Inexigibilidade

( ) Dispensa Eletrônica

( ) Dispensa sem procedimento eletrônico

Critério de Julgamento:

Menor preço global.

Metodologia de Pesquisa:

Para estimar o valor da contratação, foram utilizadas cotações feitas com fornecedores locais, junto de valores buscados no Licitacon em contratações semelhantes, mais especificamente, foi localizado contrato junto a Câmara Municipal de Getúlio Vargas. Adotou-se como critério o valor médio entre os preços coletados. Os documentos que fundamentam a pesquisa, como extratos de licitações e planilha comparativa de preços, seguem anexos a este Documento de Formalização da Demanda (DFD).

Item	Material Especificado	Qtde.	Valor máximo mensal	Valor máximo total
01	Contratação de uma solução de Firewall de próxima geração (Next-Generation Firewall - NGFW), visa proteger a rede corporativa bem como os endpoint e servidores da Prefeitura municipal de Sananduva/RS. As soluções devem proporcionar segurança, desempenho e escalabilidade adequados às necessidades da administração pública, com foco em proteção contra uma ampla gama de ameaças avançadas bem como o gerenciamento centralizado e alta disponibilidade.	12 meses	R$ 3.156,33	R$ 37.875,99

Av. Fiorentino Bacchi, nº 673 - Cep: 99840-000
Estado do Rio Grande do Sul/BR
Contato: (54) 99669-0941

DOCUMENTOS TÉCNICOS:	
Caso o produto/serviço a ser adquirido/contratado necessite de qualificação técnica específica, informar quais documentos deverão ser exigidos no Edital para que seja comprovada a habilitação do vencedor (exemplo: atestado de capacidade técnica, registro CREA/CAU/CRC, certificados de cursos específicos, etc...).	
01	Atestado de Capacidade Técnica emitida por pessoa jurídica de direito público, firmando que o licitante prestou ou presta serviços de Locação de Firewall e que cumpriu/cumpre com as obrigações assumidas, fornecido por no mínimo 01 (uma) instituição pública;
02	A empresa licitante deverá demonstrar através de declaração indicando o funcionário, que possui em seu quadro funcional no mínimo 1 (um) profissional com formação em Segurança da Informação (junto com comprovante de especialização de nível superior na área - no mínimo pós-graduação), que será o responsável técnico pelos serviços contratados;
03	Declaração indicando 1 (um) profissional com formação em CyberSecurity (junto com comprovante de especialização de nível superior na área - no mínimo pós-graduação);
04	Prova de vínculo dos profissionais com a empresa licitante, caso não possua vínculo societário, deverá apresentar a Carteira de Trabalho e Previdência Social (CTPS) com o devido registro do empregado.
05	A licitante deverá indicar, através de declaração, um responsável técnico dos serviços, de segurança virtual, devendo conter no mínimo: treinamentos em: CompTIA Security + 2, CCNA Cisco Cyberops 2, Gestão de Identidade e Acesso, Sistemas de Detecção e Prevenção de Intrusão, comprovando sua qualificação através de Certificado e/ou atestado de conclusão de cursos relacionados acima.

EXIGÊNCIAS QUANTO AO PRODUTO/SERVIÇO:	
- Caso haja exigências específicas quanto à aquisição do produto/ prestação do serviço, informar quais serão para que seja colocado no Termo de Referência (exemplo: combustíveis – necessidade de prestação de serviço 24 horas, produtos – local de entrega (para cálculo do frete), prazo de entrega ou prazo para início da prestação dos serviços, etc...) OBS: Tais exigências deverão constar também na pesquisa de preço encaminhada aos fornecedores, pois as mesmas influenciam no preço a ser cotado.	
01	A instalação, configuração, manutenção, repasse de conhecimento e suporte técnico deverá se iniciar a partir da assinatura do contrato, com um prazo máximo de 24horas para serem concluídos. Os serviços deverão ser prestados exclusivamente pela contratada, (ficando vedado a subcontratação de outra prestadora de serviço), na modalidade on-site (presencial) em todos os setores da Prefeitura Municipal de Sananduva/RS devendo ser realizada exclusivamente por técnicos especialistas e de forma presencial com tempo máximo admitido para atendimento presencial de 40 min (quarenta minutos).
02	Chamados técnicos poderão ser abertos em regime 8x5, via internet, chamada telefônica local ou discagem direta, caracterizando a abertura do chamado. Este momento será considerado o início para a contagem dos prazos estabelecidos.

Av. Fiorentino Bacchi, nº 673 - Cep: 99840-000
Estado do Rio Grande do Sul/BR
Contato: (54) 99669-0941

03	Os chamados serão registrados pela Contratada e deverão estar disponíveis para acompanhamento pela equipe da Administração Municipal, contendo data e hora da chamada, o problema ocorrido, a solução, data e hora de conclusão.
04	Os atendimentos aos chamados obrigatoriamente deverão ser realizados por profissionais certificados e deverão ser realizados presencialmente sempre que solicitado pela Administração pública, com tempo máximo de 40 (quarenta) minutos para atendimento presencial, sendo que a solução para o problema, caso seja atribuída aos equipamentos descritos, deverá ser alcançada em no máximo 24 (vinte e quatro) horas corridas após a abertura do chamado técnico.
05	Durante a execução dos serviços de suporte técnico, somente poderão ser utilizadas peças e componentes novos e originais.
06	Após a conclusão da manutenção de qualquer equipamento, a Contratada deverá gerar documento relatando as substituições de peças e componentes, contendo a identificação do chamado técnico, a data e hora do início e término do atendimento.
07	Deverá a contratada apresentar ao CONTRATANTE a certificação do profissional que irá prestar o suporte, certificação esta que deverá estar vigente durante a vigência do contrato
08	A Contratada deverá submeter o equipamento a teste de aceite técnico, realizado pela equipe de TI da Administração, a fim de comprovar o atendimento integral às especificações do edital.
09	A contratada deverá assegurar suporte técnico com SLA previamente definido em contrato, contemplando atendimento remoto imediato e prazo máximo para resolução de incidentes críticos, sob pena de aplicação de sanções.
10	A contratada será responsável por dar destinação ambientalmente adequada a resíduos eletrônicos e embalagens decorrentes da instalação e manutenção do firewall, em conformidade com a Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010).
11	É vedada a subcontratação de outra empresa para realização dos trabalhos.

Aline da Silva Ficagna

Aline da Silva Ficagna
Agente de contratação suplente conforme Portaria nº 097/2025

Av. Fiorentino Bacchi, nº 673 - Cep: 99840-000
Estado do Rio Grande do Sul/BR
Contato: (54) 99669-0941

JUSTIFICATIVA PARA ADOÇÃO DO PREGÃO NA FORMA PRESENCIAL

1. Fundamentação Legal

A presente contratação encontra respaldo no art. 28, inciso II, da Lei nº 14.133/2021, que admite o pregão como modalidade de licitação para a aquisição de bens e serviços comuns, inclusive os serviços comuns de engenharia, independentemente do valor estimado.

Ademais, o §4º do art. 17 do mesmo diploma legal dispõe que, em caráter excepcional e devidamente motivado, poderá ser adotada a forma presencial para o certame.

2. Objeto da Contratação

O objeto é a contratação de empresa especializada para fornecimento, instalação, configuração e suporte de solução integrada de segurança de rede (Firewall de Próxima Geração – NGFW), incluindo hardware, licenciamento, treinamento, suporte técnico e demais insumos necessários ao pleno funcionamento da infraestrutura de TI da Prefeitura Municipal de Sananduva/RS, conforme especificações técnicas, cronograma, pesquisa de preços e demais documentos técnicos que integram o processo licitatório.

3. Justificativa da Modalidade Presencial

a) Amplitude de participação local e regional

Considerando a natureza do objeto – aquisição de solução tecnológica para proteção de dados e continuidade dos serviços digitais –, há expectativa de participação de empresas de pequeno e médio porte da região, muitas das quais não possuem estrutura tecnológica adequada para participação em certames exclusivamente eletrônicos.

A forma presencial favorece a inclusão e amplia a competitividade, permitindo condições mais vantajosas à Administração, além de incentivar a participação de fornecedores locais e regionais, em conformidade com os princípios da economicidade e do desenvolvimento sustentável.

b) Garantia da lisura e do contraditório em tempo real

O pregão presencial assegura respostas imediatas a impugnações, pedidos de esclarecimento e recursos, com deliberações públicas e acompanhamento direto da condução do certame.

Esse formato reforça a transparência do procedimento, garante a observância do contraditório e evita falhas técnicas decorrentes de sistemas eletrônicos, comuns em localidades com conectividade instável, garantindo maior segurança e legitimidade ao processo licitatório.

c) Fiscalização social e controle institucional

A forma presencial possibilita que o certame seja acompanhado diretamente por cidadãos, órgãos de controle e interessados em geral, fortalecendo o controle social e garantindo maior publicidade e confiança no processo.

d) Adequação ao objeto e regime de contratação

Por se tratar de solução integrada (hardware, licenciamento, suporte e treinamento), a forma presencial favorece esclarecimentos técnicos imediatos durante a disputa, garantindo

Av. Fiorentino Bacchi, nº 673 - Cep: 99840-000
Estado do Rio Grande do Sul/BR
Contato: (54) 99669-0941

maior segurança tanto para a Administração quanto para os licitantes, especialmente em regime de empreitada por preço global.

4. Conclusão

Diante do exposto, considerando:

- a natureza técnica e essencial do objeto (segurança da informação e proteção de dados);
- a realidade socioeconômica e tecnológica do Município de Sananduva;
- a necessidade de garantir ampla competitividade, inclusão de fornecedores locais e regionais, transparência e lisura; e
- a adequação ao regime de empreitada por preço global.

Justifica-se plenamente a adoção do Pregão Presencial, nos termos do §4º do art. 17 da Lei Federal nº 14.133/2021, como a modalidade mais vantajosa e eficaz para atender ao interesse público na contratação pretendida.

Sananduva, 08 de setembro de 2025.

Sergio Luiz Fracasso
Secretário de Planejamento e Administração