ESP-FUND.P/CONSERV.PROD.FLORESTAL DO EST.SP

Estudo Técnico Preliminar 88/2026

1. Informações Básicas

Número do processo: 262.000023252026-10/2026

2. Descrição da necessidade

O presente Estudo Técnico Preliminar tem por objetivo a contratação de solução de TIC para acesso remoto seguro do tipo VPN, por meio de modelo de locação mensal, contemplando o fornecimento de equipamento (appliance de segurança), licenciamento e suporte técnico.

Atualmente, a instituição demanda acesso remoto seguro aos sistemas corporativos, sendo necessária a adoção de solução que garanta confidencialidade, integridade e disponibilidade das informações, bem como controle adequado de acessos.

A solução deverá contemplar:

- Fornecimento de equipamento dedicado para segurança e VPN;
- Licenciamento da solução com suporte e atualizações;
- Capacidade de acesso remoto simultâneo;
- Gerenciamento centralizado;

A contratação visa:

- Garantir acesso remoto seguro;
- Reduzir riscos de segurança da informação;
- Assegurar continuidade das atividades institucionais

3. Área requisitante

Área Requisitante	Responsável
Gerência Administrativa	Lucimara Zanetti

4. Necessidades de Negócio

A contratação de solução de VPN tem por objetivo viabilizar o acesso remoto seguro aos sistemas e recursos tecnológicos da instituição, garantindo que apenas usuários autorizados acessem a rede de forma controlada.

A solução deverá assegurar a confidencialidade e a integridade das informações trafegadas, por meio de mecanismos de criptografia e autenticação segura, prevenindo acessos indevidos.

Deverá, ainda, suportar múltiplos usuários simultâneos, com desempenho e estabilidade adequados, permitindo o trabalho remoto e o acesso externo aos sistemas institucionais sem impacto na operação.

A solução também deverá possibilitar o registro e a auditoria dos acessos, garantindo rastreabilidade das ações e atendimento às exigências de governança e à Lei Geral de Proteção de Dados (LGPD).

Dessa forma, a contratação visa reduzir riscos de segurança da informação e assegurar a continuidade das atividades institucionais.

5. Necessidades Tecnológicas

A solução de VPN a ser contratada deverá atender aos requisitos tecnológicos necessários para garantir acesso remoto seguro, desempenho adequado, continuidade dos serviços e aderência às diretrizes de segurança da informação da instituição.

5.1. Arquitetura da Solução

A solução deverá ser fornecida em modelo integrado, contemplando:

- Equipamento dedicado de segurança (appliance), novo e sem uso anterior;
- Licenciamento completo da solução durante toda a vigência contratual;
- Atualizações de segurança e firmware;
- Suporte técnico especializado.

A solução deverá operar de forma compatível com ambientes locais, em nuvem ou híbridos.

5.2. Capacidade e Desempenho

A solução deverá ser dimensionada para atender à demanda institucional, contemplando, no mínimo:

- Suporte a no mínimo **250 (duzentos e cinquenta) usuários simultâneos**;
- Throughput mínimo de **600 Mbps para tráfego VPN criptografado**;
- Estabilidade de conexões, com baixa latência e sem degradação significativa de desempenho.

O dimensionamento visa garantir continuidade das atividades e evitar gargalos operacionais.

5.3. Compatibilidade e Acesso

A solução deverá:

- Permitir acesso por **desktops, notebooks e dispositivos móveis**;
- Suportar acesso remoto seguro por múltiplos usuários simultaneamente.

5.4 Gerenciamento

Deverá ser disponibilizada interface centralizada de administração, que permita o gerenciamento eficiente da solução, incluindo a configuração de acessos, definição de políticas e acompanhamento do ambiente.

A ferramenta deverá possibilitar o monitoramento das conexões ativas em tempo real, bem como o controle das permissões de acesso, contribuindo para a governança, segurança e rastreabilidade das operações realizadas.

5.5 Disponibilidade

A solução deverá garantir alta disponibilidade do serviço, com estabilidade das conexões e desempenho adequado, de forma a não comprometer as atividades institucionais.

Deverá ainda atender a níveis mínimos de serviço, preferencialmente com disponibilidade igual ou superior a 99%, assegurando continuidade operacional e confiabilidade do acesso remoto.

5.6 Suporte Técnico

A contratada deverá fornecer suporte técnico durante toda a vigência do contrato, preferencialmente com atendimento remoto, visando a rápida resolução de incidentes e dúvidas operacionais.

Deverá também garantir a disponibilização de atualizações e correções de segurança, mantendo a solução protegida contra vulnerabilidades conhecidas.

5.7. Implantação e Configuração

Solução deverá contemplar os serviços de implantação, instalação, configuração e validação do ambiente, de forma a garantir o pleno funcionamento da solução de VPN no ambiente da CONTRATANTE. Tais serviços deverão ser executados por equipe técnica qualificada, assegurando a correta parametrização da solução, integração com a infraestrutura existente e atendimento aos requisitos de segurança da informação.

A implantação deverá incluir a configuração dos acessos remotos, definição de políticas de segurança, integração com diretório (quando aplicável) e realização de testes de funcionamento, de modo a validar a operação da solução antes de sua entrada em produção.

5.8 Documentação

A solução deverá ser acompanhada de documentação técnica completa, incluindo manuais de operação e configuração, de forma a permitir a adequada gestão pela equipe interna.

Adicionalmente, deverá ser prevista orientação ou treinamento, quando aplicável, garantindo a transferência de conhecimento e a autonomia da equipe na administração da solução.

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

6.1 Requisitos de Execução

A solução deverá ser fornecida por empresa especializada, com qualificação técnica comprovada, através de atestado de capacidade técnica comprovando fornecimento de solução de VPN, como forma de mitigar riscos associados à falha na instalação e configuração da VPN. Para tanto, deverá ser exigida a comprovação de experiência prévia da contratada e realizada validação técnica do projeto antes da implantação. A implantação assistida deverá ser prevista sempre que necessário, garantindo a correta configuração inicial da solução e reduzindo a probabilidade de paralisações, retrabalho e atrasos no início da operação. Adicionalmente, recomenda-se a realização de diagnóstico prévio da infraestrutura existente, a fim de evitar incompatibilidades técnicas e necessidade de ajustes não previstos.

6.2. Requisitos Técnicos

6.2.1 Capacidade e Dimensionamento

- Suporte a, no mínimo, 250 (duzentos e cinquenta) usuários simultâneos de VPN;
- Capacidade de processamento compatível com ambiente corporativo de médio porte;
- Throughput mínimo de 600 Mbps para conexões VPN criptografadas (IPSec ou SSL).

6.2.2. Interfaces de Rede

Possuir, no mínimo:

- 4 (quatro) interfaces Ethernet 1Gbps RJ45 para LAN e 02 (duas) para WAN;
- Suporte a interfaces adicionais (SFP ou superiores), quando aplicável;
- Possibilidade de segmentação de rede.

6.2.3. Funcionalidades de VPN

Suporte aos protocolos:

- VPN IPSec (site-to-site e acesso remoto);
- Criação e gerenciamento de no mínimo 50 (cinquenta) túneis simultâneos;
- Suporte a usuários simultâneos com estabilidade e desempenho adequado.

6.2.4. Implantação

A solução deverá contemplar:

- instalação;
- configuração inicial e integração com Active Directory da Fundação Florestal para autenticação dos usuários;
- testes de funcionamento;
- entrada em produção assistida;
- A contratada deverá garantir a correta integração com o ambiente da CONTRATANTE.

6.2.5. Autenticação e Controle de Acesso

- Integração com serviços de diretório, tais como:
- Active Directory, LDAP ou equivalente;

6.2.6. Recursos de Segurança

A solução deverá contemplar, no mínimo, os seguintes mecanismos:

- Firewall de próxima geração;
- Criptografia forte compatível com padrões atuais (AES 256 ou superior);
- Registro e armazenamento de logs de acesso e eventos de segurança;

6.2.7. Gerenciamento e Monitoramento

- Interface de gerenciamento via navegador web ou plataforma em nuvem;
- Monitoramento em tempo real das conexões e do desempenho da solução;
- Geração de relatórios operacionais e de segurança;
- Visualização de usuários conectados e sessões ativas;

6.2.8. Atualizações e Suporte

- Atualizações contínuas de firmware e assinaturas de segurança incluídas;
- Suporte técnico durante toda a vigência contratual;
- Atendimento remoto para resolução de incidentes e ajustes operacionais

6.3 Requisitos de Qualidade

A solução deverá assegurar funcionamento contínuo, com níveis adequados de desempenho, baixa latência e estabilidade das conexões, sendo essencial a realização de testes de desempenho e dimensionamento adequado antes da entrada em produção. Tais medidas visam mitigar riscos de desempenho inadequado da VPN, prevenindo lentidão no acesso aos sistemas, aumento de chamados de suporte e queda de produtividade.

6.4 Requisitos de Segurança

A solução deverá atender integralmente às diretrizes da Lei Geral de Proteção de Dados (LGPD), garantindo a confidencialidade, integridade e disponibilidade das informações trafegadas. Para mitigação de riscos de vazamento de dados e acessos indevidos, deverão ser exigidos mecanismos de segurança robustos, como criptografia forte e autenticação multifator (MFA). Adicionalmente, a solução deverá permitir controle adequado de usuários e registro de logs, possibilitando auditoria e rastreabilidade, prevenindo acessos não autorizados e reduzindo impactos decorrentes de eventuais incidentes de segurança.

6.5 Requisitos de Continuidade

A solução deverá garantir níveis mínimos de disponibilidade do serviço, formalizados em SLA, como forma de mitigar riscos de indisponibilidade da VPN, que podem comprometer o acesso remoto e a continuidade das atividades institucionais. Deverá ainda contemplar plano de contingência estruturado, prevendo ações para rápida recuperação do serviço em caso de falhas. A definição de SLA rigoroso e mecanismos de monitoramento contínuo são essenciais para assegurar a continuidade operacional e minimizar impactos na prestação de serviços.

6.6 Requisitos de Suporte

A contratada deverá prover atendimento a incidentes durante toda a vigência contratual, com definição clara de níveis de serviço (SLA), incluindo prazos de resposta e resolução. Esse requisito visa mitigar os efeitos de falhas operacionais e garantir a rápida recuperação do ambiente em situações de indisponibilidade ou mau funcionamento. O suporte deverá incluir atuação proativa na identificação de problemas, bem como correções tempestivas, reduzindo riscos de interrupções prolongadas.

6.7 Requisitos de Conformidade

A solução deverá estar em conformidade com as políticas internas de segurança da informação. Como medida de mitigação do risco de dependência excessiva do fornecedor, deverá ser exigida a entrega de documentação técnica completa e a realização de transferência de conhecimento para a equipe interna. Essas ações visam garantir maior autonomia institucional, facilitar a gestão da solução e reduzir riscos relacionados à manutenção e continuidade do serviço ao longo do tempo.

7. Estimativa da demanda - quantidade de bens e serviços

7.1 Quantidade

Item	Descrição	Quantidade
01	Solução de VPN (appliance + licenciamento + suporte	01 unidade

7.2. Premissas da Estimativa

A estimativa da demanda considera a contratação de solução de VPN em modelo de locação mensal, incluindo equipamento e licenciamento. O dimensionamento prevê atendimento a cerca de 250 usuários simultâneos, com capacidade de até 600 Mbps, garantindo desempenho e estabilidade. A solução será utilizada de forma contínua para acesso remoto seguro aos sistemas institucionais, inclusive em regime de teletrabalho.

8. Levantamento de soluções

Solução1: Serviço de VPN corporativa baseada em appliance

Foram analisadas soluções de mercado baseadas em appliance de segurança com licenciamento integrado, amplamente utilizadas em ambientes corporativos para acesso remoto seguro. As alternativas avaliadas oferecem recursos como VPN, controle de acesso, criptografia e gerenciamento centralizado, com variações em desempenho, nível de segurança e facilidade de administração. De modo geral, as soluções atendem aos requisitos técnicos e de segurança, cabendo à fase comparativa a avaliação quanto a custo, desempenho e aderência às necessidades institucionais.

Solução 2: Serviço de VPN prestado de forma gerenciada (modelo terceirizado)

Foi considerada a contratação de solução de VPN em modelo gerenciado, na qual a infraestrutura, operação, suporte e manutenção são de responsabilidade da contratada, com gestão centralizada e menor necessidade de atuação da equipe interna.

Entretanto, esse modelo apresenta menor autonomia operacional para a contratante, uma vez que ajustes e configurações dependem do fornecedor. Diante da necessidade de maior flexibilidade, agilidade e adaptação às demandas institucionais, soluções com gerenciamento próprio mostram-se mais adequadas ao ambiente da instituição.

9. Análise comparativa de soluções

As soluções analisadas apresentam dois modelos principais: serviço gerenciado e solução baseada em appliance.

No modelo gerenciado, a operação, suporte e gestão ficam sob responsabilidade da contratada, reduzindo a necessidade de atuação da equipe interna. No entanto, ajustes e configurações dependem da abertura de chamados, o que pode impactar a agilidade no atendimento de demandas específicas.

Já as soluções baseadas em appliance com licenciamento integrado oferecem maior autonomia, flexibilidade de configuração e adaptação às necessidades da CONTRATANTE.

Ambos os modelos atendem aos requisitos técnicos e de segurança, sendo a escolha da solução mais adequada condicionada ao equilíbrio entre custo, nível de segurança, capacidade de gestão e complexidade do ambiente.

10. Registro de soluções consideradas inviáveis

Durante o levantamento de soluções, foram analisadas alternativas disponíveis no mercado para atendimento à necessidade de acesso remoto seguro, incluindo diferentes modelos tecnológicos e níveis de complexidade.

Foram consideradas, inicialmente, soluções baseadas exclusivamente em software livre ou ferramentas gratuitas de VPN. Entretanto, tais alternativas foram consideradas inviáveis por não

atenderem plenamente aos requisitos institucionais de segurança, suporte técnico especializado, garantia de atualização contínua e conformidade com normas de governança e LGPD, além de demandarem maior esforço operacional da equipe interna para implantação e manutenção.

Dessa forma, foram descartadas soluções que não atendem de forma adequada aos requisitos de segurança, suporte, facilidade de gestão e custo-benefício, sendo priorizadas alternativas que ofereçam equilíbrio entre robustez técnica, simplicidade operacional e aderência à realidade institucional.

11. Análise comparativa de custos (TCO)

.

A análise de custos considerou o Custo Total de Propriedade (TCO), incluindo não apenas o valor de contratação, mas também custos de operação, suporte e manutenção ao longo do tempo.

As soluções de mercado, em geral, utilizam modelo de subscrição ou locação, garantindo previsibilidade orçamentária e evitando altos investimentos iniciais. Soluções com suporte técnico incluído reduzem riscos de indisponibilidade e custos indiretos.

Além disso, soluções com gerenciamento simplificado demandam menor esforço da equipe interna, reduzindo custos operacionais. Dessa forma, a escolha deve priorizar o melhor equilíbrio entre custo, eficiência operacional e sustentabilidade da solução.

12. Descrição da solução de TIC a ser contratada

A solução proposta consiste na contratação de VPN corporativa em modelo de locação mensal, incluindo appliance de segurança, licenciamento, implantação, suporte técnico e atualizações durante toda a vigência contratual.

O modelo adotado proporciona previsibilidade de custos, redução de investimento inicial e atualização contínua da tecnologia, alinhado às práticas de mercado.

13. Estimativa de custo total da contratação

Valor (R$): 51.602,28

A contratação é estimada em R$ 51.602,28.

14. Justificativa técnica da escolha da solução

A escolha da solução de VPN em modelo de locação mensal baseia-se na análise técnica das alternativas de mercado, considerando critérios de segurança, desempenho, escalabilidade e facilidade de gestão.

A solução selecionada apresenta equilíbrio entre robustez e simplicidade operacional, sendo adequada à capacidade da equipe técnica. Além disso, o gerenciamento centralizado facilita a administração e reduz a complexidade do ambiente.

O modelo de locação, com suporte e atualizações incluídos, garante previsibilidade orçamentária e manutenção contínua da solução.

15. Justificativa econômica da escolha da solução

A escolha da solução em modelo de locação mensal demonstra-se economicamente vantajosa, considerando o custo total de propriedade (TCO) ao longo da vigência contratual. Diferentemente de modelos baseados na aquisição de equipamentos e licenças permanentes, a locação permite a diluição dos custos em parcelas mensais, reduzindo a necessidade de investimento inicial elevado.

Além disso, o modelo adotado contempla, de forma integrada, o fornecimento do equipamento, licenciamento, suporte técnico e atualizações de segurança, eliminando custos adicionais que poderiam surgir em modelos fragmentados de contratação. Tal abordagem proporciona maior previsibilidade orçamentária e facilita o planejamento financeiro da instituição.

Dessa forma, conclui-se que a solução adotada apresenta o melhor equilíbrio entre custo, benefício e sustentabilidade ao longo do tempo, atendendo aos princípios da eficiência, economicidade e interesse público.

16. Benefícios a serem alcançados com a contratação

A contratação da solução de VPN corporativa proporcionará maior segurança no acesso remoto, com comunicação criptografada e controle de acesso, em conformidade com a LGPD.

Garantirá a continuidade dos serviços, com acesso estável aos sistemas institucionais, inclusive em trabalho remoto.

Também permitirá maior governança e rastreabilidade das operações, por meio de registros e auditoria de acessos, além de melhorar a eficiência operacional da área de TI, com gerenciamento simplificado e suporte técnico contínuo.

Adicionalmente, o modelo adotado assegura previsibilidade orçamentária, atualização tecnológica e modernização da infraestrutura, alinhada às boas práticas de segurança da informação.

17. Providências a serem Adotadas

Para viabilizar a contratação, a Administração deverá:

- Elaborar o Termo de Referência com especificações técnicas, requisitos de segurança e níveis de serviço (SLA);
- Realizar pesquisa de preços;
- Definir a modalidade de contratação conforme a legislação vigente;
- Instruir o processo administrativo com a documentação necessária;

- Disponibilizar a infraestrutura para implantação da solução;
- Acompanhar tecnicamente a execução contratual;
- Realizar testes e validação da solução após a implantação.

Essas providências visam garantir a contratação de forma planejada, eficiente e em conformidade com a legislação.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

A contratação é viável técnica e economicamente, pois a solução atende às necessidades de acesso remoto seguro, garantindo segurança, desempenho e disponibilidade.

Do ponto de vista técnico, está aderente aos requisitos e contribui para a mitigação de riscos operacionais. Sob o aspecto econômico, o modelo de locação mensal oferece previsibilidade de custos, redução de investimento inicial e inclusão de suporte e atualizações.

A solução é compatível com a infraestrutura existente e adequada à capacidade da equipe, sendo necessária e vantajosa para a Administração.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

OCTAVIO DE OLIVEIRA LOPES

Equipe de apoio

Assinou eletronicamente em 14/04/2026 às 17:44:11.