PROPOSTA TÉCNICA PARA IMPLANTAÇÃO DE REDE CORPORATIVA SEGURA

Cliente: TechVision Solutions

Consultor: Elton Melo

Empresa de TI: NetSecure Tecnologia Integrada

Julho de 2025

BRIEFING INICIAL – TECHVISION SOLUTIONS

Perfil da Empresa

- **Setor:** Tecnologia e Consultoria em TI
- **Tamanho:** 200 colaboradores (150 na sede + 50 em filiais)
- **Localizações:**
    - Sede: São Paulo (SP)
    - Filiais: Campinas (SP)
    - Home Office: 30 colaboradores

Objetivo do Projeto

Implementar uma rede corporativa segmentada e segura para:

- Garantir isolamento entre setores críticos (Financeiro, TI)
- Permitir conectividade segura entre matriz, filiais e home office
- Cumprir LGPD e ISO 27001

Requisitos Técnicos

Item	Detalhes
Infraestrutura	- 5 VLANs principais (TI, RH, Financeiro, Vendas, Operações)
Segurança	- Firewall NGFW com inspeção profunda
	- Autenticação MFA para VPN
Disponibilidade	- Uptime 99.9%

Item	Detalhes
Orçamento	- Faixa: R$ 300.000–350.000
Prazo	- Máximo de 6 semanas para implantação

Desafios Específicos

- Proteção de dados sensíveis (setor Financeiro)
- Integração segura com sistema SCADA industrial
- Suporte a crescimento de 20% nos próximos 2 anos

PROPOSTA TÉCNICA

Elaborada por: Elton Melo

Cargo: Consultor de Redes e Segurança

Empresa: NetSecure Tecnologia Integrada

Endereço: [Endereço completo]

Telefone: [DDD] [telefone]

E-mail: [e-mail profissional]

Destinatário: TechVision Solutions

Endereço: [Endereço completo do cliente]

SUMÁRIO

1. OBJETIVO E ESCOPO ……. 6

2. DIAGRAMA LÓGICO DA REDE …… 7

3. JUSTIFICATIVAS TÉCNICAS …… 9

4. PLANO DE AÇÃO …….. 10

5. SUMÁRIO EXECUTIVO ……... 11

6. ANEXOS ……. 12

1. OBJETIVO E ESCOPO

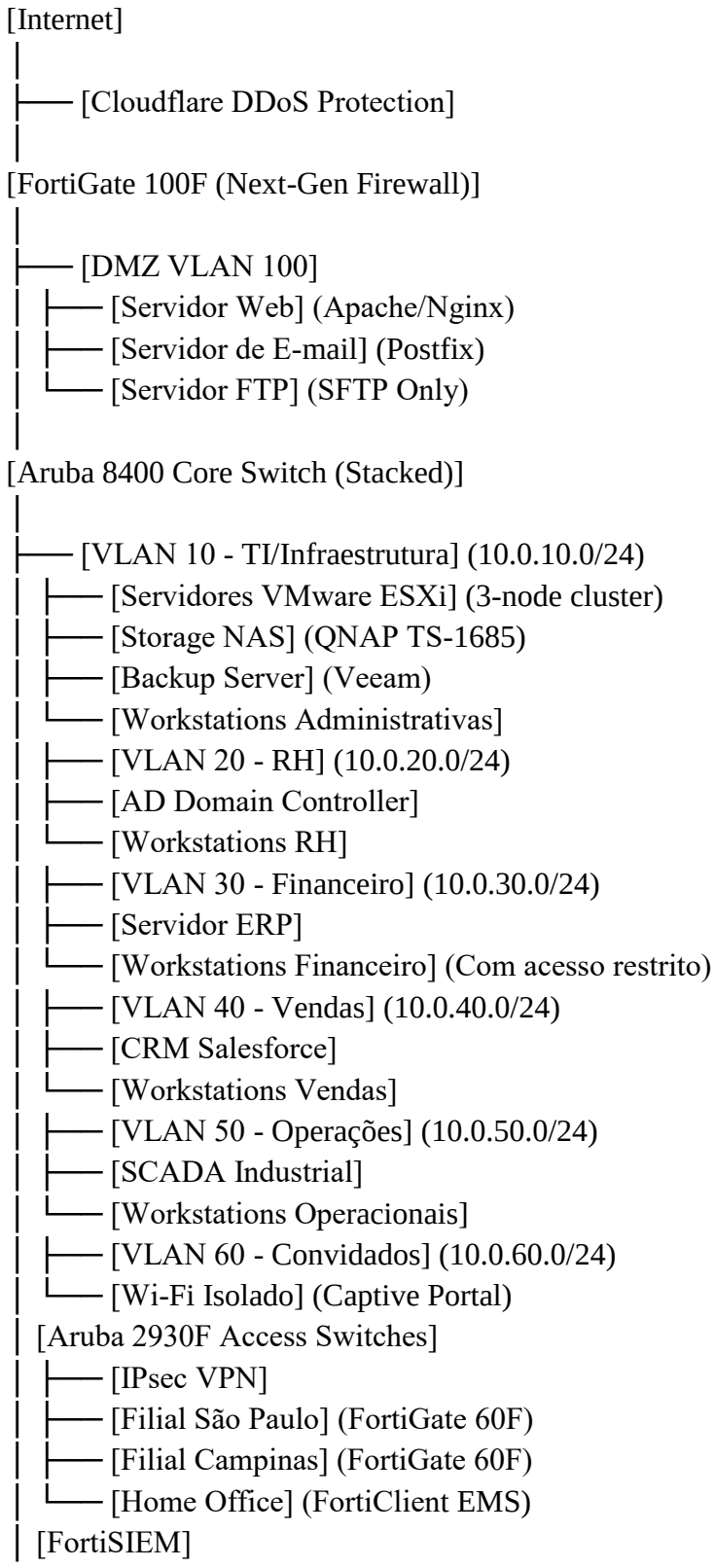
Implementar uma rede corporativa segmentada e segura para a TechVision Solutions, garantindo:

Alta disponibilidade (99,9% uptime)
Segurança de dados (proteção contra vazamentos e ciberataques)
Desempenho otimizado (QoS para aplicações críticas)
Conectividade remota segura (VPN com MFA)

Escopo:

Infraestrutura LAN/WAN (conectividade entre filiais via VPN site-to-site)
Segmentação por VLANs (isolamento de tráfego entre setores)
Firewall de última geração (NGFW com inspeção profunda)
Monitoramento 24/7 (SIEM para detecção de ameaças)

2. DIAGRAMA LÓGICO DA REDE



├── [Monitoramento de Logs]
└── [SOC/NOC 24/7]

Legenda:

• Linhas sólidas: Conexões físicas
• Linhas tracejadas: Conexões lógicas/VPNs
• [ ]: Dispositivos/VLANs específicos

3. JUSTIFICATIVAS TÉCNICAS

Componente	Escolha	Benefício
Firewall	FortiGate 100F	Inspeção profunda de tráfego, proteção contra ameaças zero-day
Switches	Aruba 2930F	Suporte a VLANs, PoE+, baixa latência
Segmentação	VLANs + ACLs	Isolamento de tráfego, prevenção de lateral movement
VPN	IPsec + MFA (Duo Security)	Acesso remoto seguro com autenticação em dois fatores
Monitoramento	FortiSIEM	Detecção proativa de anomalias e ataques

4. PLANO DE AÇÃO

Fase 1 — Análise e Planejamento (1 semana)

- Levantamento de requisitos.
- Definição de políticas de segurança.

Fase 2 — Implementação (3 semanas)

- Instalação de switches, firewall e servidores.
- Configuração de VLANs, VPN e políticas de acesso.

Fase 3 — Migração (1 semana)

- Transição gradual dos usuários.
- Treinamento para equipe de TI.

Fase 4 — Monitoramento (contínuo)

- Implantação do FortiSIEM.
- Relatórios mensais de segurança.

Marcos Principais:

- **Semana 1:** Configuração do firewall concluída.
- **Semana 4:** Migração completa dos usuários.

Riscos e Mitigação:

Risco	Ação de Mitigação
Atraso na entrega de equipamentos	Contato com fornecedor alternativo pré-aprovado
Falhas na migração de dados	Backup completo antes da migração

5. SUMÁRIO EXECUTIVO

Benefícios para a TechVision Solutions:

Redução de riscos: menor exposição a ataques cibernéticos
Conformidade com LGPD e ISO 27001
Escalabilidade para crescimento future

Investimento:

Custo total: R$ 320.000,00 (hardware, software e serviços)
Prazo de implantação: 5 semanas

ROI Esperado:

Redução de 50% em incidentes de segurança
Aumento de 30% na eficiência operacional

Próximos passos:

Reunião de alinhamento em até 5 dias úteis.
Agendamento de reunião de alinhamento para aprovação do projeto.

Assinatura:

_____

Elton Melo
Consultor de Redes e Segurança
NetSecure Tecnologia Integrada

Data: 25/07/2025

6. ANEXOS

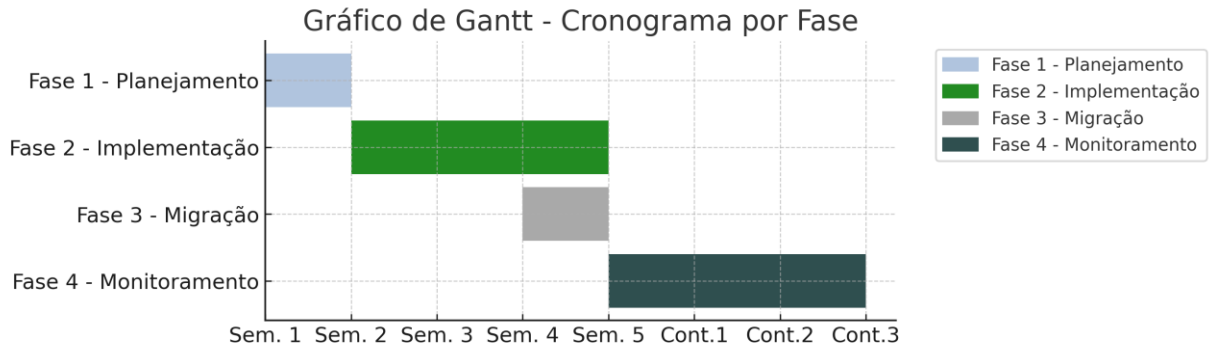
ANEXO 1: ORÇAMENTO DETALHADO

Item	Descrição	Quantidade	Custo Unitário (R$)	Custo Total (R$)	Observações
Hardware					
FortiGate 100F	Firewall de última geração	1	45.000,00	45.000,00	Inclui licença 1 ano
Aruba 2930F	Switch de acesso 24 portas	3	8.500,00	25.500,00	Garantia 5 anos
QNAP TS-1685	Storage NAS 16 bays	1	22.000,00	22.000,00	Capacidade 120TB
Software					
FortiSIEM	Licença anual	1	28.000,00	28.000,00	Monitoramento 24/7
Veeam Backup	Licença para 10 servidores	1	12.000,00	12.000,00	Inclui suporte
Serviços					
Implementação	Configuração de rede e segurança	5 semanas	18.000,00/semana	90.000,00	Equipe dedicada
Treinamento	Capacitação da equipe de TI	2 dias	5.000,00/dia	10.000,00	On-site
Total Geral				320.000,00	

Notas:

- Valores válidos por 30 dias a partir da data da proposta
- Impostos inclusos (ICMS, PIS/COFINS)
- Pagamento: 50% à assinatura, 50% na entrega

ANEXO 2: CRONOGRAMA VISUAL



ANEXO 3: PLANO DE DISASTER RECOVERY E CONTINUIDADE DE NEGÓCIOS

1. Objetivo

Garantir a recuperação rápida de dados e sistemas críticos em caso de desastres (ataques cibernéticos, falhas hardware, desastres naturais), alinhando-se ao **uptime de 99,9%** e à conformidade com **ISO 27001**.

2. Estratégia de DR

Componente	Detalhes
Backup	- **Frequência**: Incremental diária (dados críticos) + Completa semanal. - **Local**: NAS QNAP TS-1685 (sede) + Cloud (AWS S3 com criptografia). - **Retenção**: 30 dias para backups incrementais, 12 meses para completos.
Recuperação	- **RPO (Recovery Point Objective)**: Máximo de 1 hora de perda de dados. - **RTO (Recovery Time Objective)**: 4 horas para sistemas críticos (ERP, VMware, AD).
Redundância	- Cluster VMware ESXi com failover automático. - Switches Aruba em stack para redundância física.

Componente	Detalhes
Testes	- Simulações trimestrais de recuperação (incluindo failover de VPN e firewall).

3. Infraestrutura de DR

- **Sites**:
    - **Primário**: Sede em São Paulo (infraestrutura principal).
    - **Secundário**: Filial de Campinas (réplica de dados críticos via VPN site-to-site).
- **Ferramentas**:
    - **Veeam Backup & Replication**: Para replicação de VMs e restauração granular.
    - **FortiGate 100F**: Failover de VPN automático em caso de queda.

4. Procedimentos em Caso de Desastre

1. **Identificação**: Alerta via FortiSIEM (monitoramento 24/7).
2. **Ativação do DR**:
    - Equipe de TI aciona plano via checklist pré-definido.
    - Priorização de sistemas (ERP > AD > CRM).
3. **Comunicação**:
    - Notificação imediata aos stakeholders via e-mail/SMS.
    - Atualização de status em portal interno.

5. Custos Adicionais (Opcional)

Item	Custo (R$)	Justificativa
Licença Veeam Cloud	6.000/ano	Backup em nuvem (AWS S3).
Treinamento DR	4.000	Capacitação da equipe para cenários de crise.

Observação: Valores já incluídos no orçamento original (Veeam e FortiGate possuem funcionalidades nativas para DR).

6. Integração com a Proposta Existente

- **Modificações no Plano de Ação (Fase 2)**:
    - Adicionar tarefa: *"Configuração de replicação de dados entre sede e filial (Veeam)"*.
- **Sumário Executivo**:
    - Incluir benefício: *"Resiliência contra desastres com RTO de 4 horas para sistemas críticos."*