PROTOCOLO DE SERVIÇO

Rede Privada Fibra Ótica

Sumário

Rede Privada Fibra Ótica

Justificativa e Objetivos do Serviço

Os parâmetros que regem a economia atual fazem necessária a modernização da gestão pública através da interligação das entidades governamentais.

Além disso, o acesso à rede de comunicação de alta velocidade é essencial para o desenvolvimento econômico nos dias atuais, uma vez que o acesso à banda larga possibilita a efetiva utilização de recursos, como a integração entre instituições e empresas; integração entre instituições governamentais; a possibilidade de serviços de governo eletrônico (*e-gov*); a redução de custos; serviços de melhor qualidade e com maior disponibilidade; o aumento da segurança da informação, uma vez que a maior parte do tráfego ocorrerá dentro da rede de domínio do Estado e não na Internet; a eficiência da máquina governamental através de aplicações e soluções desenvolvidas, baseadas na utilização da rede disponível; a comunicação e o compartilhamento de dados entre os diversos órgãos que compõem a estrutura governamental; entre outros recursos possíveis.

A adoção do serviço objetiva resolver questões como:

- A modernização da gestão pública: possibilidade de publicação de serviços eletrônicos do governo à população; possibilidade de criação de soluções de atendimento e acompanhamento de serviços online pelos cidadãos;
- A criação da infraestrutura necessária para o oferecimento de outras soluções para o Governo, como VoIP interno, modernização de unidades de saúde com a implantação da Telemedicina, pontos de Tele Vigilância, bancos de dados governamentais centralizados;
- A redução nos custos: com a possibilidade de utilização de meios de comunicação internos (VoIP) que reduzirão os custos com chamadas interurbanas, por exemplo; a possibilidade de utilização de soluções de videoconferência, que reduzirão gastos com viagens e aditarão agilidade nas resoluções de questões essenciais à governabilidade; a redução do tempo para a execução das tarefas, com dados centralizados e conexão de qualidade com a Internet, com melhora no desempenho do funcionalismo público e dos serviços aos cidadãos, tornando menos onerosas as ofertas de serviços do governo;
- Conexões com maior qualidade e disponibilidade: conexões locais, interligando os órgãos a bases de dados centralizadas, com redundância de link, maior velocidade (banda) e maior disponibilidade;

- Possibilidade de incentivo ao Turismo: os centros turísticos terão maior acesso à divulgação e propaganda de seus atrativos; possibilidade de criação de aplicativos de cunho turístico ou que incentive o comércio do Estado do Piauí;
- O pleno desenvolvimento do estado através dos meios tecnológicos, culturais, turísticos, educacionais, econômicos, comerciais e autossustentáveis, promovendo interconexão aos órgãos estaduais.

Requisitos Gerais

Cada localidade (unidade do Governo do Estado) para onde for contratada a Rede Privada através da tecnologia de Fibra Ótica, será conectada à rede estadual de alta velocidade com a possibilidade de trafegar dados com o Datacenter e com outros pontos que possuírem o mesmo serviço, sem a necessidade de utilizar a Internet para os conteúdos disponíveis nos pontos acessíveis (Datacenter ou pontos com o serviço de Rede Privada contratado).

As taxas de transferência possíveis, síncronas entre *download* e *upload* estão relacionadas a seguir:

- 10 Mbps;
- 20 Mbps;
- 30 Mbps;
- 50 Mbps;
- 100 Mbps;
- 200 Mbps;
- 300 Mbps;
- 500 Mbps;
- 1 Gbps.

Solução de Segurança Lógica (*Firewall*)

Serão aplicados pelo menos três níveis de Segurança Digital para a Rede Privada:

1. *Core* da rede: solução de segurança redundante e com alta disponibilidade, responsável pela segurança do perímetro; tal solução será acomodada na Sala Cofre do Datacenter;
2. Pontos de Distribuição: solução de segurança responsável pelo perímetro que conecta cada uma das cidades à rede de alta capacidade do Estado; tal solução será acomodada nos racks de cada cidade;

3. Pontos de Acesso: solução de segurança responsável pelo perímetro entre os usuários finais e a rede de Distribuição; tal solução deverá ser acomodada em cada entidade atendida.

As soluções se segurança digital serão dimensionadas de acordo com: os serviços entregues, as demandas de cada localidade ou cidade e com a demanda total da rede. Devem ser soluções com hardware específico para a solução, com software integrado (*firmware*), especificamente projetado para fornecer um recurso de computação específico (*appliance*).

A fim de garantir a segurança, o controle e a alta disponibilidade, as soluções ofertadas deverão atender, no mínimo, às seguintes funcionalidades:

FILTRO DE APLICAÇÕES: Deve permitir inspeção profunda de pacotes (DPI - *Deep Packet Inspection*) que proporciona recursos avançados de segurança e filtragem de dados, deve permitir o bloqueio de aplicativos peer 2 peer. Deve ser capaz de preservar as informações das entidades estaduais e prevenir contra invasões;

IDS/IPS: A solução deve ser capaz de detectar o tráfego de dados, com uma base com, no mínimo, vinte mil assinaturas de ataques;

VPN: Com este recurso, usuários do Estado poderão ter acesso remoto seguro à sua via computador, tablet ou celular, mesmo estando na Internet. A VPN estabelece um túnel com a rede remota que mantém seus dados seguros enquanto eles trafegam pela rede. Ao utilizar uma VPN é possível se conectar de forma segura e até mesmo transmitir informações protegidas em redes públicas, graças à utilização de criptografia. Este recurso ainda permite VPN Failover, que realiza a verificação de links específicos e permite que o administrador configure rotas seguras quando algum desses links ficar inativo. Deverá ser possível a criação de túneis criptografados entre as diversas entidades governamentais e o *loadbalance* de VPN;

***FAILOVER* DE REGRAS**: A solução deve ofertar uma funcionalidade que define conteúdos (ou origem-destino) prioritários de tráfego de rede ao habilitar ou desabilitar automaticamente túneis VPN (IPSEC) e regras de filtragem, caso a conexão principal fique inativa. Com esta funcionalidade é possível manter, por exemplo, o ERP ou sistema de pagamento funcionando e desabilitar o acesso à internet, caso o link de internet fique inativo. Ou ainda, mudar uma regra de priorização de tráfego (QoS) para um determinado serviço;

BALANCEAMENTO DE LINK: A solução ofertada deve disponibilizar recurso de alta disponibilidade e tolerância a falhas em múltiplos links. A solução deve prever o melhor desempenho da rede ao permitir o balanceamento de link por políticas, oferecendo pelo menos três modos diferentes para realizá-lo:

1. Link Failover: Esta tecnologia permite o monitoramento do link principal, enquanto o link secundário fica inativo. A vantagem desta tecnologia é que ela economiza o link secundário, pois este só ficará ativo se o link principal falhar;

CLUSTER: A rede deverá ser mantida tolerante a falhas, com alto desempenho, disponibilidade e escalabilidade (possibilidade de expansão). Com o cluster, os recursos da rede serão mantidos em funcionamento de forma eficiente e em tempo integral. Ao conectar dois *firewalls* à rede e replicar suas configurações, é possível manter a rede segura 24 horas por dia e realizar a substituição imediata caso um deles pare de funcionar, sem afetar o desempenho da sua rede e sem perda de informações;

LINK *AGGREGATION*: Com este protocolo é possível criar uma forma padronizada para agrupar múltiplos links entre ativos (equipamentos de camada 2) fazendo que estes se comportem como se fossem um único link, aumentando a capacidade de transferência de dados (*throughput* de rede) do link na comunicação. A técnica de Link *Aggregation* ainda fornece redundância caso um dos links venha a falhar;

QoS: Deverá ser possível classificar os tipos de serviço da rede por grau de relevância e otimizar o tráfego de dados da rede com a funcionalidade QoS (Qualidade de Serviço). A qualidade de serviço é o tratamento diferenciado do tráfego reunido em classes de serviço, com o objetivo de garantir o nível de serviço adequado a cada aplicação. Assim, em caso de congestionamento, será possível priorizar determinados fluxos ou aplicações.

Materiais que serão utilizados

ITEM	DESCRIÇÃO	PARÂMETROS
1	Fibra ótica (*backbone core*)	Conforme Termo de Referência.
2	Fibra ótica (*backbone* de distribuição)	Conforme Termo de Referência.
3	Ativos de rede *core*	Conforme Termo de Referência.
4	Ativos de rede distribuição	Conforme Termo de Referência.
5	Ativos para infraestrutura de rede de acesso	De acordo com a necessidade contratada e completamente compatível com a Rede de Acesso.
6	Ativos para segurança lógica	Que atendam as demandas descritas neste documento.
7	Datacenter com Sala Cofre	Conforme Termo de Referência.

8	Centro de Operações da Rede (COR) com Centro de Comando e Controle, Sala de Crise, Suporte e Inteligência, Atendimento e Administração	Conforme Termo de Referência.
9	Solução de Software para Gerenciamento da Rede (NMS)	Conforme Termo de Referência.
10	Miscelâneas para ativação completa da solução	Todos os itens necessários para compor a solução dentro das características exigidas.

Principais itens do serviço

Serviço de Rede Privada através do uso de tecnologia de Fibra Ótica, com, no mínimo, as seguintes opções de contratação de banda: 10 Mbps, 20 Mbps; 30 Mbps; 50 Mbps; 100 Mbps; 200 Mbps; 300 Mbps; 500 Mbps e 1 Gbps.

Segurança Digital para os dados trafegados na Rede Privada.

Medidores de desempenho

Deve ser possível a extração de relatórios de:

- Síntese de utilização da Rede Privada:
  - Total;
  - Por Cidade;
  - Por Localidade;
- Quantidade de paradas nos serviços de Rede Privada;
- Tempo da parada ao início do atendimento pela equipe de campo;
- Tempo total da parada até a resolução e reestabelecimento do serviço;
- Motivo da parada;
- Resolução: configurações, substituição de equipamentos, etc.

Após a ativação dos serviços de Rede Privada, deverão ser emitidos relatórios que comprovem a disponibilidade de banda de acordo com o que foi contratado.

O atendimento no Centro de Operações de Rede deverá possuir canais livres de comunicação (telefone, ramal VoIP, e-mail ou interface Web para abertura de chamados), em regime 24/7 (24

horas por dia e 7 dias por semana) e o tempo máximo para a primeira resposta (informando sobre a ciência do incidente e o tempo previsto para resolução) deve ser de 2 horas.

O tempo total da parada ao reestabelecimento do acesso à Internet deve ser de até 24 (vinte e quatro) horas, considerando o regime 24/7 (24 horas por dia e 7 dias por semana).

Em caso de vandalismo, interrupção longa ou permanente da energia elétrica e paradas ocorridas por motivos que fogem à governança da Concessionária, a parada e o tempo de resolução não serão contabilizados dentro dos critérios de desempenho do serviço. Nestes casos, o relatório mensal deverá explicitar de forma clara que o motivo foge à governança da Concessionária. É responsabilidade do Estado garantir a Segurança Pública.

Periodicamente serão aplicados questionários de satisfação aos usuários a fim de que a Concessionária tenha condições de otimizar ou corrigir a entrega dos serviços.

O desempenho do serviço de Rede Privada - Fibra Ótica entregue, por fim, será medido por:

- Tempo médio da primeira resposta para os chamados;
- Tempo médio de solução para os problemas;
- Efetividade no atendimento aos chamados;
- Percentual de reabertura de chamados;
- Disponibilidade do serviço;
- Quantidade de não conformidades nas instalações dos pontos de atendimento;
- Quantidade de não conformidades na manutenção e conservação nos pontos de atendimento;
- Percentual de entrega de banda de Rede Privada utilizando Fibra Ótica.

Qualificação Técnica

Para a coordenação da instalação e ativação dos pontos de Serviços de Conexão à Internet serão necessários profissionais Técnicos em Telecomunicações ou equivalentes, com experiência comprovada em Fibra Ótica.

Os profissionais responsáveis pela instalação deverão ser certificados nas normas ABNT NR10 e NR35, quando exigíveis.

Responsabilidades

Do Poder Concedente:

- Auxiliar a Concessionária na emissão das licenças e autorizações necessárias, quando exigíveis;
- A segurança contra vandalismo e questões de Segurança Pública que fogem à governança da Concessionária;
- Contatar a central de atendimentos no COR a fim de informar problemas, incidentes ou tirar dúvidas e acompanhar a resolução do que foi relatado;
- Participar das pesquisas de satisfação aplicadas;
- Solicitar a emissão de relatórios de desempenho;
- Garantir o fornecimento de energia elétrica nas localidades (unidades do Governo) para os equipamentos envolvidos na entrega dos serviços.

Da Concessionária:

- Instalar e manter em funcionamento os itens: Backbone *Core*, Backbone de Distribuição, Backbone de Acesso, Datacenter, Centro de Operações de Rede com Software de Gerenciamento (NMS) e Serviços de Conexão à Internet;
- Manter uma central de atendimento em regime 24/7 (24 horas por dia e 7 dias por semana) para resolução de problemas, incidentes e dúvidas;
- Aplicar pesquisas de satisfação dos usuários;
- Emitir relatórios de desempenho e utilização da infraestrutura quando solicitados pelo Governo do Estado;
- Validar junto ao Governo do Estado os locais de instalação para emissão de licenças e autorizações, caso necessárias;
- Registrar, acompanhar e finalizar junto aos órgãos competentes, como o CREA, as obras ou serviços executados;
- Obter e manter as licenças e autorizações necessárias à Concessionária, quando cabíveis;
- A segurança e sigilo dos dados trafegados na rede, exceto em questão de segurança que fogem à governança da Concessionária. Neste caso, explicitar detalhadamente a falha na segurança.
- Fornecimento de protocolos de acesso as bases de dados dos serviços(Como leitura) para o monitoramento em tempo real dos serviços, bem como para criação de painéis gerenciais, pelas próprias ferramentas de monitoramento de B.I do Estado, sem necessidade de solicitação a concessionaria. Isso visa a autonomia do Estado e da Agencia de Tecnologia da

Informação de manter o controle do serviço prestado, bem como do repasse das informações para poder concedente

Do Poder Concedente e Concessionária:

- O Poder Concedente e a Concessionária não medirão esforços a fim de certificar a segurança dos dados dos usuários e conteúdos trafegados, porém não é possível garantir que o acesso a dados ou dispositivos, oriundo do uso inadequado ou mal-intencionado de usuários, mantenham-se sigilosos, uma vez que vírus, descuidos pessoais, inabilidade ou mal-uso podem causar a interceptação dos mesmos;
- O Poder Concedente e a Concessionária também não medirão esforços em entregar serviços de qualidade aos usuários, porém não poderão ser responsabilizadas por nenhum dano ao usuário causado por inabilidade ou mau uso da Rede Privada;
- A Concessionária não será responsabilizada por danos causados ao Poder Concedente por mal-uso, inabilidade ou má intenção no uso da Rede Privada proveniente dos usuários.