Fundo Nacional de Desenvolvimento da Educação - FNDE

Audiência Pública nº 3/2018

Link de Conectividade do Programa de Inovação Educação Conectada

OBJETO

Constitui objeto desta especificação técnica contratação de serviço de link de dados/internet de alta velocidade (banda larga) para escolas públicas brasileiras, atendendo ao Programa de Inovação Educação Conectada.

O serviço pretendido compreende a entrega, instalação, configuração, manutenção e sustentação de sinal de internet banda larga para as escolas, garantindo disponibilidade, integridade, autenticidade e velocidade de acesso à rede mundial de computadores.

(*) A infraestrutura interna de acesso à internet não é objeto desta contratação.

Serviço de link de dados/internet de alta velocidade (banda larga)

1. Considerações Gerais

1.1. A unidade de medida utilizada para aferição de serviço prestado será disponibilidade de link;
1.2. Para fins de pagamento será considerada a média de velocidade efetivamente entregue e a disponibilidade de serviço;
1.3. Para fins de atendimento do Programa de Inovação Educação Conectada, é recomendado que se calcule, no mínimo 100 Kbps por aluno conectado.
1.4. As tabelas abaixo apresentam o total de escolas por faixa de conexão e região.

Conexões por Infraestrutura	Escolas região Norte
Até 200	314
Até 500	1589
Até 1000	753
>1001	344

Conexões por Infraestrutura	Escolas região Nordeste
Até 200	1065
Até 500	5063
Até 1000	1628
>1001	482

Conexões por Infraestrutura	Escolas região Sul
Até 200	988
Até 500	2054
Até 1000	1124
>1001	366

Conexões por Infraestrutura	Escolas região Sudeste
Até 200	1049
Até 500	4092
Até 1000	4142
>1001	1825

Conexões por Infraestrutura	Escolas região Centro-Oeste
Até 200	173
Até 500	853
Até 1000	565
>1001	281

Total de escolas Urbanas: 22.250
Total de alunos: 15 Milhões
Total de professores: 581 mil

(Fonte: censo 2017)

2. DAS ESPECIFICAÇÕES DO SERVIÇO

2.1. Para atender o objetivo desta contratação o serviço deverá:

2.1.1. Ser dimensionado de acordo com o Plano Pedagógico do ente contratante e ter como limitador a quantidade de alunos matriculados na escola, professores e funcionários cadastrados;

2.1.2. O serviço de link de internet deverá ser prestado pela CONTRATADA no regime de 24x7x365 (24 horas por dia, 7 dias por semana, 365 dias no ano);

2.1.3. Será de responsabilidade da CONTRATADA fornecer todos os equipamentos e meios necessários à plena prestação do serviço, excluindo-se o fornecimento de energia elétrica para alimentação dos equipamentos nas dependências das unidades, o aterramento da rede e a climatização das dependências.

2.1.4. Fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os equipamentos/recursos que forem necessários (roteadores, modens, racks, estações de gerenciamento, meios de transmissão, cabeamento, acessórios necessários e outros) para o provimento do serviço, conforme solicitado nesta especificação. Os equipamentos serão de propriedade da CONTRATADA, que deverá ser responsável pelo suporte técnico destes.

2.1.5. Garantir que a disponibilidade, a segurança, o desempenho e a qualidade do serviço prestado esteja dentro dos limiares estabelecidos pela CONTRATANTE.

2.1.6. A largura de banda deve sempre estar disponível na totalidade do fluxo contratado.

2.1.7. Caso solicitado, a CONTRATADA deverá realizar alterações nas taxas de transmissão contratadas, com a adequação dos recursos necessários (roteadores, enlaces, backbone e outros) garantindo o alto desempenho do serviço.

2.1.8. Os circuitos empregados pela CONTRATADA deverão atender às Normas Técnicas Brasileiras e regulamentações da ANATEL, quando essas não entrarem em conflito com o especificado neste documento.

2.1.9. Manter o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas ao serviço de telecomunicação contratado.

2.1.10. Aplicar e manter atualizados os patches de segurança nos seus roteadores ou em outros equipamentos, de sua rede, os quais são exclusivos para a prestação do serviço à CONTRATANTE.

3. MODEM/ROTEADOR

3.1. Os roteadores deverão ser fornecidos, instalados, mantidos, gerenciados e operados pela CONTRATADA com a garantia, o desempenho e os níveis de serviços contratados. Cada roteador será fornecido com todos os acessórios e programas necessários à sua instalação, operação e monitoração (cabo de console, cabo de alimentação, cabo V35 e outros cabos e acessórios que se fizerem necessários).

3.2. Todos os roteadores suportarão, além dos protocolos básicos para operação em uma rede IP, Frame Relay e PPP, com compressão de dados e o protocolo de roteamento OSPF. Com opção de security telnet e IP security (IPSec).

3.3. Os roteadores terão facilidades de configuração através de porta serial e da console de monitoramento.

3.4. O roteador de acesso à Internet e o roteador do circuito deverão ter as seguintes configurações mínimas:

3.4.1. Possuir, no mínimo, 03 (três) portas de LAN GigaBit ethernet com conector tipo RJ45 para cabos UTP e que seja compatível com o padrão IEEE 802.3;

3.4.2. Possuir opção de boot local e permitir armazenamento de firmware e configuração em memória compact flash que deverá ser fornecida caso seja necessário;

3.4.3. Possuir no mínimo 256 MB de memória flash ou similar e 2048 MB de memória DRAM, permitindo que o equipamento atenda a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do fabricante;

3.4.4. Possuir seu firmware e sistema operacional em versão que atenda a todos os requisitos mínimos necessários (memória, flash, dentre outros) para suportá-lo;

3.4.5. Suportar o protocolo de rede IP sobre ATM, compatível com a RFC 2684;

3.4.6. Suportar portas seriais Síncronas, Assíncronas, ATM OC3 e Gigabit;

3.4.7. Implementar os protocolos de roteamento OSPF (Open Shortest Path First) e BGP 4;

3.4.8. Implementar o protocolo de distribuição de endereços IP - DHCP Relay, Server, Client;

3.4.9. Implementar o protocolo protocolo IGMPv1, v2 e v3 (Internet Grouping Message Protocol), PIM-SM e PIM-DM;

3.4.10. Implementar os protocolos de gerenciamento SNMP V1, V2, V3 (Simple Network Management Protocol), empregando a MIB-II (Management Information Base), RMON (Remote Monitoring);

3.4.11. Implementar, no mínimo, 32 VLAN (Virtual Local Area Network), com base em portas, endereços MAC e Padrão IEEE 802.1q;

3.4.12. Implementar NAT (Network Address Translation) e PAT (Port Address Translation);

3.4.13. Suportar os padrões: QoS (Quality-of-Service), 802.1p e 802.1q;

3.4.14. Disponibilizar, no mínimo, três níveis de senha de acesso;

3.4.15. Deve possuir arquitetura modular, permitindo a substituição de interfaces e do módulo de processamento central;

3.4.16. Capacidade de comutação mínima de 1.400 (mil e quatrocentos) kbps disponível no equipamento;

3.4.17. Permitir a criação de funções de filtragem baseada em listas de controle de acesso com capacidade de filtrar através de endereços de origem e destino e porta UDP e TCP de origem e destino (ACL Básicas e Estendidas - Lista de controle de acesso) 3 mil linhas;

3.4.18. Devem ser do mesmo fabricante e compartilhar a mesma sintaxe de comandos dos demais roteadores fornecidos;

3.4.19. Devem possuir interfaces com velocidades iguais ou superiores às especificadas para os links fornecidos;

3.4.20. Permitir a configuração remota através de TELNET, SSH e por porta de console padrão RS-232 ou porta console RJ-45. O equipamento deverá possuir, além da porta console, porta auxiliar que permita a ligação de modem externo;

3.4.21. Deverá ser compatível com, pelo menos, um dos protocolos a seguir: NetFlow, NetStream ou IPFIX, de forma a permitir estatísticas mais apuradas do tráfego;

3.4.22. Implementar IPSEC com criptografia em hardware. Devem ser suportados 1500 túneis externos IPSEC simultâneos, com capacidade mínima de 8 Mbps de tráfego criptografado em 3DES/MD5, considerando-se pacotes de 1400 bytes;

3.4.23. Deve implementar a criação de tuneis VPN dinamicamente, de forma a garantir que escritórios remotos criem túneis entre si sob demanda, mesmo quando associados a endereços IP dinâmicos;

4. CONTROLE DE TRÁFEGO E GERENCIAMENTO

4.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo (tais como: youtube, ustream, etc) e ter um alto consumo de largura de banda, 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, tanto de áudio como de vídeo streaming.

4.2. Suportar a criação de políticas de QoS por:

4.2.1. Endereço de origem;

4.2.2. Endereço de destino;

4.2.3. Por usuário e grupo do LDAP/AD;

4.2.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

4.2.5. Por porta;

4.3. O QoS deve possibilitar a definição de classes por:

4.3.1. Banda Garantida;

4.3.2. Banda Máxima;

4.3.3. Fila de Prioridade;

4.4. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

4.5. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

4.6. Disponibilizar estatísticas RealTime para classes de QoS;

4.7. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário;

4.8. Permitir a criação de filtros para arquivos e dados pré-definidos;

4.9. Os arquivos devem ser identificados por extensão e assinaturas;

4.10. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);

4.11. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.12. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

4.13. Permitir listar o número de aplicações suportadas para controle de dados;

4.14. Permitir listar o número de tipos de arquivos suportados para controle de dados;

4.15. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento.

4.16. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

4.17. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

4.18. O gerenciamento deve permitir/possuir:

4.18.1. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

4.18.2. Criação e administração de políticas de Filtro de URL;

4.18.3. Monitoração de logs;

4.18.4. Ferramentas de investigação de logs;

4.18.5. Debugging;

4.18.6. Captura de pacotes;

4.18.7. Acesso concorrente de administradores;

4.18.8. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.18.9. Deve permitir o uso de palavras chaves e cores para facilitar a identificação de regras;

4.18.10. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN client-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas;

4.18.11. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

4.18.12. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

4.18.13. Autenticação integrada ao Microsoft Active Directory e servidor Radius;

4.18.14. Localização de quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

4.18.15. Deve atribuir sequencialmente um número a cada regra de NAT, QOS e regras de DOS;

4.18.16. Criação de regras que fiquem ativas em horário definido;

4.18.17. Criação de regras com data de expiração;

4.18.18. Backup das configurações e rollback de configuração para a última configuração salva;

4.18.19. Suportar rollback de Sistema Operacional para a última versão local;

4.18.20. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

4.18.21. Validação de regras antes da aplicação.

4.19. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

4.20. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

4.21. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)

4.22. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

4.23. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

4.24. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

4.25. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

4.26. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

4.27. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

4.28. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;

4.29. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

4.30. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;

4.31. Deve ser possível exportar os logs em CSV;

4.32. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

4.33. Rotação do log;

4.34. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

4.35. Situação do dispositivo e do cluster;

4.36. Principais aplicações;

4.37. Principais aplicações por risco;

4.38. Administradores autenticados na gerência da plataforma de segurança;

4.39. Número de sessões simultâneas;

4.40. Status das interfaces;

4.41. Uso de CPU;

4.42. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

4.43. Resumo gráfico de aplicações utilizadas;

4.44. Principais aplicações por utilização de largura de banda de entrada e saída;

4.45. Principais aplicações por taxa de transferência de bytes;

4.46. Principais hosts por número de ameaças identificadas;

4.47. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;

4.48. Deve permitir a criação de relatórios personalizados;

4.49. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

4.50. Gerar alertas automáticos via:

4.50.1. Email;

4.50.2. SNMP;

4.50.3. Syslog;

5. MÉTRICAS PARA MONITORAMENTO

5.1. Todos os equipamentos devem ser homologados para possibilitar a instalação de firmware do SIMET BOX, oferecido pelo NIC.br com o objetivo de analisar a qualidade da Internet.

5.2. Medições realizadas pelo Simet Box:

5.2.1. Número médio de conexões simultâneas realizadas no mês;

5.2.2. Disponibilidades dos ativos (histórico e percentual);

5.2.3. Throughput;

5.2.4. Consumo de banda input e output;

5.2.5. Quality of service;

5.2.6. Emissão de Relatórios em PDF ou XML;

5.2.7. Disponibilidade do acesso à Internet;

5.2.8. Traceroute;

5.2.9. Vazão TCP e UDP;

5.2.10. Jitter;

5.2.11. Latência;

5.2.12. Perda de pacotes.

6. SLA

O tempo início e conclusão do atendimento deverá seguir o estabelecido na tabela de classificação de chamado abaixo:

Tabela de classificação de Chamado				
Severidade	Descrição	Tempo de início de atendimento	Tempo de solução a menos de 20 KM da sede do município	Tempo de solução a mais de 20 KM da sede do município
1 – Urgente	Indisponibilidade do serviço.	Em até uma hora	Em até duas horas	Em até três horas
2 – Muito Importante	Erros ou problemas reincidentes que impactam no serviço.	Em até duas horas	Em até quatro horas	Em até seis horas
3 – Importante	Manutenção dos equipamentos que suportam o serviço.	Em até quatro horas	Em até doze horas	Em até vinte e quatro horas
4 – Informação	Consulta técnica, dúvidas em geral, monitoramento e gerenciamento da infraestrutura.	Em até quatro horas	Em até dezesseis horas	Em até trinta e duas horas

7. SUPORTE TÉCNICO

7.1. O suporte será realizado sempre que solicitado pela unidade educacional por meio da abertura de chamado técnico diretamente à empresa contratada via central de atendimento:

7.2. Suporte Remoto – serviço de atendimento durante o horário comercial, em português, aos chamados técnicos, executados via central de atendimento;

7.3. Suporte Local – serviço de atendimento local a chamados técnicos críticos, que deverão ser atendidos presencialmente, por profissional capacitado. Este serviço terá acionamento 24x7;

7.4. Suporte ao Serviço - desinstalação, reconfiguração ou reinstalação decorrentes de falhas nos ativos ou necessidades no negócio, atualização da versão, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados realizado fora do horário comercial, se remotamente.

7.5. O suporte será realizado sempre que solicitado pela unidade educacional por meio da abertura de chamado técnico diretamente à empresa contratada via central de atendimento;

7.6. Todas as solicitações feitas pelo contratante deverão ser registradas pela contratada em sistema de atendimento, disponibilizado pela contratada, para acompanhamento e controle da execução dos serviços;

7.7. Cada chamado pela CONTRATANTE deverá ser registrado no sistema de atendimento e disponibilizado de forma clara, compreensível e facilmente legível, devendo compreender as seguintes informações mínimas:

7.7.1. Número de registro de abertura do chamado técnico;

7.7.2. Data e hora de abertura do chamado técnico;

7.7.3. Identificação do Ponto de Presença que apresenta a falha/interrupção;

7.7.4. Identificação do funcionário responsável pela abertura do chamado;

7.7.5. Solicitante;

7.7.6. Descrição do problema apresentado;

7.7.7. Status da solicitação (chamado em aberto, pendentes ou fechados);

7.7.8. Responsável pela execução do serviço de normalização do ponto;

7.7.9. Data e hora da execução dos serviços necessários;

7.7.10. Data e hora do encerramento do chamado.

7.8. A execução dos serviços que demandarem a interrupção da prestação do serviço de link de internet somente poderá ser realizada mediante prévia autorização da unidade escolar.

7.9. Para a realização dos serviços de suporte técnico on-site, a contratante permitirá o acesso dos técnicos habilitados e identificados da contratada à escola. Esses técnicos ficarão sujeitos a todas as normas internas da unidade escolar inclusive aquelas referentes à identificação, trajes, trânsito e permanência em suas dependências.

7.10. Um chamado técnico somente poderá ser fechado após confirmação do contratante do término do atendimento;

7.11. A contratada após a realização dos serviços de suporte técnico deverá apresentar um relatório de visita, contendo identificação do chamado, data e hora de abertura do chamado, data e hora do início e término do atendimento, identificação do defeito, técnico responsável pela solução, as providências adotadas e outras informações pertinentes.

7.12. O tempo início e conclusão do atendimento deverá seguir o estabelecido na tabela de classificação de chamado abaixo, não devendo ultrapassar os prazos estabelecidos para as respectivas severidades:

8. COMPATIBILIDADE E CERTIFICAÇÕES

8.1. Certificações que o modelo ofertado deverá possuir: ANATEL e FCC;

8.2. Todos os opcionais deverão ser homologados pelo fabricante do equipamento;

9. PROVISIONAMENTO:

Deverá possibilitar que os equipamentos possam ser entregues provisionados para o domínio educacional (incluir o domínio definido).

10. EMBALAGEM DOS EQUIPAMENTOS

Para efeitos de descarte correto, deverão as embalagens (papelão, plástico, isopor, outros) possuir identificação do nível de reciclagem, devendo esta estar em conformidade com as normas da ABNT.