**Termo de Referência para a Contratação de Serviços Tecnológicos Educacionais em atendimento aos municípios consorciados ao CIM-Jequitinhonha**

**1. OBJETO**

1.1. Registro de Preços para contratação de (i) Serviços de valor adicionado (SVA) prestados a partir do licenciamento para uso da **Plataforma Tecnológica de Conectividade Gerenciável e Segura** com fins exclusivamente educacionais, na modalidade PaaS (Plataform as a Service), (ii) prestação de serviços de **suporte técnico presencial** e (iii) **locação de modens WI-FI portáteis**, para viabilização das atividades pedagógicas remotas disponibilizadas pelos municípios integrantes ao CIM-JEQUITINHONHA.

**2. NATUREZA DO OBJETO**

2.1. Objeto de mesma natureza é entendido como aquele do mesmo ramo de atividade, e considera-se ramo de atividade a linha de fornecimento consignada ao fornecedor, observada a classe de materiais e/ou serviços vinculadas ao objeto deste Termo de Referência.

**3. PRAZO DO CONTRATO/ATA DE REGISTRO DE PREÇOS E PRORROGAÇÃO**

3.1. O prazo de vigência da Ata de Registro de Preços será de 1 (um) ano, sujeito a prorrogação por igual período, de acordo com as normativas aplicáveis.

**4. FUNDAMENTAÇÃO DA CONTRATAÇÃO**

4.1. Esta contratação, baseada no ETP anexo aos autos, visa atender à necessidade de fornecer plataforma tecnológica às escolas municipais, assegurando condições adequadas para o acesso ao ensino, conforme diretrizes educacionais.

**5. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO**

5.1. Conforme levantamento prévio, identificou-se a necessidade de contratar uma plataforma tecnológica para atender às especificidades de cada escola municipal, visando melhorar e promover a qualidade do ensino, conforme detalhado abaixo e anexo a este Termo de Referência:

# 5.2. Topologia da Solução:

5.2.1. A CONTRATADA será responsável por toda a infraestrutura tecnológica desde o fornecimento dos dispositivos de acesso, os meios de acesso ao conteúdo, filtros de acesso e as infraestruturas técnicas de processamento, de segurança e de privacidade dos usuários.

5.2.2. Todo o tráfego de dados demandados pelos usuários deverá ser direcionado e processado pela **Plataforma Tecnológica de Conectividade Gerenciável e Segura** da CONTRATADA, neste documento chamada de ***PLATAFORMA***. Esta *PLATAFORMA* realizará os filtros de conteúdo ou restrições de acesso aplicáveis a cada perfil de usuário, (aluno por série, professor ou servidor administrativo), de acordo com as autorizações definidas pela equipe da Secretaria no momento do cadastro de cada usuário envolvido ou contemplado.

5.2.3. O dispositivo de acesso, componente que irá viabilizar a identificação dos usuários e o acesso à *PLATAFORMA*, permitindo que o aluno ou professor tenha acesso às ferramentas, conteúdo e Internet de qualquer local, desde que esteja sob área de cobertura de uma das redes de conectividade habilitadas pela CONTRATADA. Por meio do dispositivo de acesso o aluno terá acesso restrito e controlado às ferramentas de conteúdo e educação remota e à Internet, sempre seguindo as regras de acesso definidas pela CONTRATANTE.

5.2.4. A *PLATAFORMA* fornecida pela CONTRATADA realizará toda a checagem de autorização permitindo o acesso dos usuários apenas ao conteúdo online autorizados ou aos servidores de conteúdo digital adotados pelas Secretarias de Educação. Toda política de acesso será definida pela CONTRATANTE e implementada pela CONTRATADA.

5.2.5. A *PLATAFORMA* deve estar munida de equipamentos (hardwares) e softwares capazes de processar todo o tráfego demandado pelos usuários da CONTRATANTE, gerir todos os filtros e armazenar todos os logs para posterior criação de dashboards e relatórios como demonstrado na Figura 1, e para isso deve ser composta pelos componentes especificados no ANEXO I.



*Figura 1: Topologia da solução.*

5.2.6. A CONTRATADA deverá ainda prover a locação de modens Wi-Fi portáteis para atendimento aos professores, de forma que tais profissionais possam dispor de uma rede Wi-Fi para conexão dos dispositivos utilizados durante o processo educacional. A rede Wi-Fi oferecida deverá seguir os padrões técnicos de mercado, ter a mobilidade e a portabilidade necessária para viabilizar a conectividade dos diversos dispositivos utilizados pelos professores (notebooks, chromebooks, smart TVs, smartphones, dentre outros). Nos modens Wi-Fi portáteis serão incluídos os dispositivos de acesso contratados para atendimento aos professores, de forma que a conectividade gerenciada e controlada possa ser acessada dos diversos dispositivos utilizados pelo professor.

5.2.7. Além da *PLATAFORMA* e dos Modens Wi-Fi portáteis, a CONTRATADA deverá prestar serviços de suporte técnico presencial com o objetivo de apoiar a área pedagógica das Secretarias Municipais de Educação na implementação dos programas de educação remota.

# 5.3. Descrição detalhada do objeto:

## A *PLATAFORMA* é fruto de uma integração e composta por dispositivos de hardware, softwares e serviços técnicos especializados com o objetivo de permitir o acesso aos recursos de educação remota, fornecidos pela Secretaria de Educação do município para alunos e servidores.

## A *PLATAFORMA* compreende uma solução tecnológica, resultado da integração de diversas ferramentas e tecnologias, com operação em nuvem (*cloud computing*), e está classificada em órgãos a exemplo da ANATEL como um SVA – Serviço de Valor Adicionado, de forma que não é requerido às Licitantes as homologações, autorizações ou certificações para exploração de serviços específicos de telecomunicações, tais como SMP – Serviço Móvel Pessoal.

## Como parte integrante do objeto consta, ainda, a locação de equipamentos tipo Modens Wi-Fi portáteis e serviços de suporte tecnológico especializado na *PLATAFORMA*.

## Este certame licitatório tem como objetivo a contratação, em lote único, por critério de seleção de menor preço para os seguintes itens:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ITEM** | **DESCRIÇÃO** | **UNIDADE** | **QUANT.** | **PRAZO (meses)** |
| 1 | LICENÇAS DE USO DE PLATAFORMA TECNOLÓGICA EM CLOUD COMPUTING (PAAS) COM RECURSOS GESTÃO, CONTROLE, CONECTIVIDADE MÓVEL E CYBER SEGURANÇA PARA VIABILIZAR O ACESSO DE **ALUNOS** ÀS FERRAMENTAS DE ENSINO REMOTO.  LICENÇA ANUAL COM CAPACIDADE DE PROCESSAMENTO DE 60 GB/ANO. | LICENÇA DE USO ANUAL  (SUBSCRIÇÃO) | 34.830 | N/A |
| 2 | LICENÇAS DE USO DE PLATAFORMA TECNOLÓGICA EM CLOUD COMPUTING (PAAS) COM RECURSOS GESTÃO, CONTROLE, CONECTIVIDADE MÓVEL E CYBER SEGURANÇA PARA VIABILIZAR O ACESSO DE **PROFESSORES** ÀS FERRAMENTAS DE ENSINO REMOTO.  LICENÇA ANUAL COM CAPACIDADE DE PROCESSAMENTO DE 120 GB/ANO. | LICENÇA DE USO ANUAL  (SUBSCRIÇÃO) | 800 | N/A |
| 3 | MODEM WI-FI PORTÁTIL | LOCAÇÃO / MÊS | 800 | 12 |
| 4 | SUPORTE TECNOLÓGICO PRESENCIAL – TIPO 1 | HORA TÉCNICA / MÊS | 500 | 12 |
| 5 | SUPORTE TECNOLÓGICO PRESENCIAL – TIPO 2 | HORA TÉCNICA / MÊS | 1000 | 12 |

* 1. **Plataforma de Gestão e Controle dos Acessos e Conectividade (*PLATAFORMA):***
     1. A *PLATAFORMA* é uma solução composta por hardware, software e serviços técnicos especializados que devem ser fornecidos pela CONTRATADA em infraestrutura própria sem necessidade de qualquer tipo de contratação de infraestrutura por parte da CONTRATANTE.
     2. A *PLATAFORMA* deve permitir a criação de perfis de usuários em acordo com a necessidade da CONTRATANTE, onde estarão todas as parametrizações e eventuais customizações necessárias para acesso ao conteúdo por parte dos alunos, professores e colaboradores das Secretarias de Educação.
     3. Os Perfis de usuários deverão possuir lista de liberação de acesso (whitelist) específicos. Cada série/ano da educação básica deverá possuir um respectivo Perfil válido para todos os alunos desta série.
     4. Os Professores deverão possuir Perfil específico, com acesso gerenciado e controlado a partir de uma lista de endereços bloqueados (blacklist).
     5. A *PLATAFORMA* fornecido pela CONTRATADA deverá disponibilizar um ambiente WEB com possibilidade de inclusão e visualização de, no mínimo, os seguintes campos de para cadastramento de dados:
        1. Das escolas: Nome da escola, Endereço completo da escola, Gestor da escola, E-mail do gestor da escola e Diretor da escola;
        2. Das turmas: Nome da escola, Série/Ano e Número da turma;
        3. Dos alunos: Nome da escola, Série, Ano letivo, Número da turma, Nome do aluno, Matrícula, Ano de nascimento e Endereço.
     6. A *PLATAFORMA* deve possuir sistema de varredura e auditoria de inconsistências nos dados fornecidos pela CONTRATANTE, apresentando:
        1. Relatório de cadastros duplicados ou aluno com mais de um cadastro.
        2. Relatório de cadastros incompletos.
        3. Relatório de duplicidade em turmas e escolas.
        4. Para o caso de duplicidade ou inconsistência nos cadastros o sistema deve apresentar alarme informando o erro, para que medidas cabíveis possam ser tomadas.
     7. A CONTRATADA deve possuir equipe técnica especializada na parametrização da *PLATAFORMA* que será responsável por incluir o Banco de Dados disponibilizado e exportado pela CONTRATANTE.
     8. Os requisitos técnicos mínimos da *PLATAFORMA* estão especificados no ANEXO I e as funcionalidades básicas estão detalhadas neste item.
     9. A *PLATAFORMA* deve possuir integrado à sua infraestrutura e aos bancos de dados um aplicativo ou ambiente web para que a equipe da CONTRATANTE realize a ativação dos dispositivos de acesso.
     10. Características Gerais da *PLATAFORMA*:
         1. Deve possuir mecanismos de gerenciamento de senhas, expiração, bloqueio, alteração, reset, histórico dos colaboradores, alunos e professores das secretarias de educação.
         2. Deve permitir mecanismos de extração, transformação e carga de dados.
         3. Todas as aplicações e infraestrutura tecnológica necessária para o pleno funcionamento da *PLATAFORMA* devem estar instaladas em Data Center com certificação TIER III disponibilizado pela CONTRATADA conforme especificado no Anexo I.
         4. A *PLATAFORMA* deve possuir 4 tipos de Perfis de Utilização: Administrador, Professor, Aluno e Cadastrador Detalhados a seguir
            1. O Perfil de Utilização Administrador será utilizado pela CONTRATADA para realizar criação e parametrização dos usuários no módulo de Gerenciamento de acordo com os Perfis de Utilização definidos.
            2. O Perfil de Utilização Professor será utilizado pela CONTRATANTE e deve permitir a visualização dos endereços de acesso (urls e aplicativos) ao conteúdo e materiais definidos pelas Secretarias de Educação e visualização dos conteúdos de todas as turmas de responsabilidade do professor.
            3. O Perfil de Utilização Aluno deve permitir a visualização do conteúdo definido para sua respectiva turma e matéria.
            4. O Perfil de Utilização Cadastrador terá apenas acesso ao APP ou ambiente WEB e seus menus suspensos que possuirão as informações pré-definidas por meio das parametrizações dos bancos de dados fornecidos pela CONTRATANTE.
         5. A *PLATAFORMA* deve permitir aos gestores da CONTRATANTE realizar manutenção do cadastro a qualquer momento pós-implantação da solução, permitindo editar todos os itens referentes às etapas dos cadastramentos, essas manutenções deverão ser executadas pelo Service Desk da CONTRATADA.
         6. A *PLATAFORMA* é responsável por garantir a conectividade ao conteúdo acessado pelos alunos seja o definido pelas regras de segurança das Secretarias de Educação.
         7. A *PLATAFORMA* deve monitorar os Dispositivos de Acesso.
         8. A *PLATAFORMA* deve permitir a inserção, retirada e edição dos endereços de conteúdo a serem disponibilizados aos alunos, de acordo com os Perfis de Utilização pré-definidos pela CONTRATANTE. Essas retiradas e edições devem ser executadas pelo Service Desk da CONTRATADA por meio de Ordem de Serviço aberta pela CONTRATANTE.
         9. A *PLATAFORMA* deve registrar todas as alterações realizadas na lista de conteúdo, registrando quem fez a alteração, a data, o horário e qual conteúdo foi adicionado, retirado ou atualizado.
         10. A *PLATAFORMA* deve permitir inserir os dias da semana e horários em que o conteúdo estará liberado para acesso dos alunos.
         11. A definição dos dias e horários só deve ser permitida para a lista de conteúdos de forma única, não sendo possível atribuir dias e horários diferentes para as diversas opções da lista.
         12. Deve conter filtros na tela de acesso com o intuito de facilitar a pesquisa e visualização dos conteúdos.
         13. Deve possuir aplicação instalada no dispositivo de acesso a fim de garantir o encaminhamento do tráfego de acordo com as regras pré-estabelecidas, com isso o aluno só deve ter acesso ao conteúdo pré-definido em perfil.
         14. Todos os dados de status, localização e nível de utilização do dispositivo de acesso e do volume de consumo de internet devem ser consolidados em relatórios diários, semanais e mensais.
         15. A plataforma deve permitir a geração de mapa de calor exibindo a concentração de Dispositivos de Acesso de acordo com a última localização para cada Dispositivo de Acesso.
         16. O mapa de calor gerado deve possibilitar a aproximação e distanciamento na sua visualização, e possuir escala de cores para concentração dos Dispositivo de Acesso.
         17. Deve gerar alarmes de usuários com utilização fora do compliance definido, permitindo ações da CONTRATANTE seja com alunos, professores ou servidores da Secretaria de Educação.
         18. Deve possibilitar a restrição de forma automática do uso do Dispositivo de Acesso sempre que ferir regras do compliance ou a pedido da CONTRATANTE.
         19. A Plataforma deve possuir menu no dashboard com no mínimo as seguintes opções, relacionadas ao gerenciamento dos Dispositivos de Acesso:
             1. Bloquear Dispositivo de Acesso.
             2. Reativar Dispositivo de Acesso.
             3. Suspender Dispositivo de Acesso.
             4. Cancelar Dispositivo de Acesso.
             5. Troca de ICCID.
             6. Substituir Dispositivo de Acesso.
             7. Migrar proprietário do Dispositivo de Acesso.
             8. Informações do cliente.
             9. Manutenção de quarentena.
     11. Do aplicativo ou ambiente web fornecido pela CONTRATADA
         1. Deve consultar o banco de dados parametrizado na etapa de implantação trazendo automaticamente em formato de menu suspenso as informações de escola, turma e aluno, e devem possuir as seguintes funcionalidades:
            1. No caso de APP ser compatível com os sistemas operacionais Android e iOS.
            2. No caso de Web ser compatível com os principais navegadores de mercado.
            3. Permitir a identificação e preenchimento automáticos dos dados dos Dispositivos de Acesso através da leitura dos seus códigos de barras ou QR Code.
            4. Possuir campos digitáveis para inserção dos códigos de forma manual, quando necessário.
            5. Deve exigir credenciais de acesso aos cadastradores e liberar a vinculação apenas dos alunos cujas turmas foram definidas para o mesmo.
            6. Trazer as opções de escola, séries/ano, turmas e nome do aluno.
     12. Implantação e Ativação da *PLATAFORMA*:
         1. A implantação e ativação da *PLATAFORMA* é um serviço realizado pela CONTRATADA no início do projeto composto por parametrização e preparação do ambiente de TI (CLOUD). Trata-se de um serviço realizado unicamente, no início da prestação dos serviços do Contrato.
         2. A implantação e ativação da *PLATAFORMA* é o serviço responsável por viabilizar tecnicamente o cadastramento de todos os alunos, professores e dos componentes que permitem a conexão ao ambiente tecnológico de educação remota.
         3. Para o serviço de implantação e ativação da *PLATAFORMA* a CONTRATADA deverá:
            1. Levantar e parametrizar os requisitos de segurança e acesso dos alunos, professores e demais colaboradores da CONTRATANTE;
            2. Levantar e parametrizar escolas, matérias, séries, turmas, alunos, gestores, diretores e professores que participarão da educação remota, criando um perfil específico para cada série da educação básica contemplada com os dispositivos.
            3. Para a parametrização da solução a CONTRATANTE disponibilizará à CONTRATADA um banco de dados e/ou planilha eletrônica ou arquivo .csv com informações de escolas, séries, turmas, alunos, professores e demais servidores que serão contemplados com os Dispositivos de Acesso.
  2. **Dispositivo de Acesso (chip):**
     1. O Dispositivo de Acesso é o instrumento por meio do qual o aluno terá acesso à *PLATAFORMA*. Estes serão disponibilizados pela CONTRATADA aos alunos e professores da rede municipal, que poderão inseri-lo nos equipamentos/dispositivos móveis, tais como, tablets, smartphones ou modens portáteis.
     2. O Dispositivo de Acesso fornecido pela CONTRATADA deve realizar a conexão à *PLATAFORMA* por meio das redes de telefonia móveis (3G ou 4G) de, pelo menos, 02 das operadoras de telefonia móvel atuantes nacionalmente e nas localidades, priorizando sempre a operadora com melhor infraestrutura de conectividade (sinal de cobertura).
     3. O Dispositivo de Acesso fornecido deve conectar o tablet ou smartphone dos usuários (alunos ou professores) e os modens Wi-fi portáteis à *PLATAFORMA,* queprocessará as demandas de acesso via Internet e conectará o aluno ao conteúdo digital desejado e autorizado. O acesso dos usuários à rede educacional deve ser direto e restrito ao perfil definido pelas Secretarias de Educação dos Municípios.
     4. O Dispositivo de Acesso deverá ser ativado por equipe da CONTRATADA, após recebimento de solicitação formal enviada pela equipe da CONTRATANTE habilitada para tal.
     5. Da Ativação do Dispositivo de Acesso:
        1. A CONTRATADA deve realizar treinamento com equipe definida pela CONTRATANTE demonstrando por meio de videoaulas e presencialmente, quando necessário, os passos para cadastramento dos alunos por meio do aplicativo ou ambiente web da *PLATAFORMA*.
     6. O Dispositivo de Acesso deve ser disponibilizado lacrado e configurado para permitir conectividade limitada aos usuários, permitindo acesso apenas a conteúdos contidos na política de segurança das Secretarias de Educação.
     7. O Dispositivo de Acesso será distribuído aos alunos e professores pela CONTRATANTE por meio das escolas da rede.
  3. A *PLATAFORMA* deverá manter a conectividade de alunos e professores dentro de níveis de serviços estabelecidos neste documento e será prestado pelo período de 12 meses após a ativação do serviço, prazo de validade da licença de uso de PaaS em questão.
  4. A licença de subscrição é um item de vigência e duração anual (12 meses) após ativação oficial junto à CONTRATADA, composto por mão de obra técnica especializada para o suporte e manutenção da *PLATAFORMA* fornecida pela CONTRATADA e atualização e manutenção do cadastro dos alunos e professores.
     1. A Contratada deverá garantir que a *PLATAFORMA* tenha capacidade de processamento 60 GB por ano para cada dispositivo de acesso ativado para alunos e capacidade de processamento 120 GB por ano para cada dispositivo de acesso ativado para professores e, além de oferecer a possibilidade de configuração/parametrização das regras de distribuição mensal destas capacidades contratadas ao longo dos meses de vigência da licença de uso (12 meses).
     2. A CONTRATADAdeve identificar a operadora de telefonia móvel que melhor atenda a localidade onde os usuários irão utilizar o serviço da *PLATAFORMA* e habilitar o dispositivo de acesso com a melhor qualidade de sinal possível, dentre as 02 Operadoras de SMP selecionadas.
     3. A *PLATAFORMA* deve permitir a gestão de utilização dos pacotes de dados disponibilizados aos usuários via os dispositivos de acesso.
     4. A *PLATAFORMA* deve permitir a realização da mudança do provedor de conectividade ou da operadora de telefonia móvel de forma remota (sem troca do chip/dispositivo móvel), a partir de um comando eletrônico da central de monitoramento da CONTRATADA.
     5. Os comandos à distância para execução da substituição remota dos provedores de conectividade ou da operadora de telefonia móvel deverão seguir um protocolo definido e aprovado pela CONTRATANTE na fase de implantação da *PLATAFORMA*;
     6. Para troca de operadora a CONTRATADA deve seguir critérios de melhor cobertura em cada localidade onde o aluno ou professor estiver acessando a plataforma educacional das Secretarias.
     7. A CONTRATADA deve considerar, para efeito de dimensionamento e precificação de sua proposta comercial, um volume anual total de substituição do provedor de conectividade ou da operadora móvel a ser realizada pela CONTRATADA, o limite de até 15% do total de dispositivos de acesso ativados pela CONTRATANTE.
     8. O serviço da CONTRATADA deve possuir Service Desk para atendimento aos colaboradores das Secretarias de Educação envolvidos no projeto. O Service Desk deve tirar dúvidas e auxiliar o colaborador em processos relacionados ao serviço contratado.
     9. O Service Desk não fará atendimento a alunos e professores, trata-se de um canal de comunicação exclusivo entre a CONTRATADA e os colaboradores definidos pelas Secretarias de Educação para gestão da *PLATAFORMA*.
     10. A CONTRATADA deverá manter durante toda vigência do contrato um profissional devidamente treinado na *PLATAFORMA* e capaz de auxiliar e suportar os colaboradores da CONTRATANTE no que for necessário para a melhor utilização da *PLATAFORMA*.
  5. Detalhamento dos Serviços de suporte inclusos no licenciamento da *PLATAFORMA*:
     1. A CONTRATADA deve possuir equipe para realizar o monitoramento dos Dispositivos de Acesso e spare parts para realizar troca de itens sempre que defeitos de fabricação forem identificados. Além disso, deve manter em estoque mínimo de 5% do total de dispositivos de acesso ativados para trocas exigidas pelo projeto.
     2. A CONTRATADA será responsável pela conexão LAN TO LAN entre as estruturas das operadoras de telefonia móvel e o Data Center onde a *PLATAFORMA* for instalada.
     3. A conexão LAN TO LAN deve estar adequada à necessidade de acessos simultâneos totais por turno manhã, tarde e noite.
     4. É de responsabilidade da CONTRATADA possuir equipe capacitada para desenvolver, parametrizar, customizar e manter a *PLATAFORMA* e toda infraestrutura funcional dentro dos padrões e níveis de serviço exigidos neste Termo de Referência e seus anexos.
     5. A CONTRATADA deve disponibilizar gestor de projetos responsável por coordenar e supervisionar a implantação da solução, e acompanhar o projeto após sua implantação até o fim do contrato.
     6. Quando do fornecimento dos aplicativos móveis e aplicações a serem utilizados pelos usuários colaboradores da CONTRATANTE no processo de educação remota, a instalação destas ferramentas será de responsabilidade da CONTRATANTE.
     7. A CONTRATANTE ficará responsável pela definição da lista de sites/links (urls), aplicativos ou portais de conteúdo a serem liberados para acesso pelos usuários contemplados.
     8. É de responsabilidade da CONTRATADA a realização de assistência técnica corretiva de todos os componentes da *PLATAFORMA*.
     9. A CONTRATADA deve disponibilizar acesso online aos relatórios de atendimentos corretivos.
     10. É de responsabilidade da CONTRATADA executar atividades de programação, manutenção preventiva e corretiva da *PLATAFORMA*, garantindo o cumprimento das normas e níveis de serviços. Tais atividades são:
         1. Identificar e corrigir falhas na *PLATAFORMA*;
         2. Executar alterações de configurações;
         3. Instalar, configurar e manter softwares da solução;
         4. Monitorar os serviços, infraestrutura de TI e demais sistemas e aplicações que compõem a *PLATAFORMA*;
         5. Fazer backup das configurações da *PLATAFORMA*;
         6. Verificar redundância e failover dos componentes da *PLATAFORMA*;
         7. Fazer checklist diário do funcionamento da *PLATAFORMA*;
         8. Executar rotina de testes;
         9. Verificar logs;
         10. Testar conexões;
         11. Avaliar interfaces dos Dispositivos de Acesso;
         12. Avaliar as condições de funcionamento da *PLATAFORMA*.
     11. A CONTRATADA deve comprovar proficiência da equipe de analistas de administração e suporte da *PLATAFORMA* a ser gerenciada e mantida.
     12. A CONTRATADA deve disponibilizar atendimento em conformidade com o nível de serviço informado neste Termo de Referência.
     13. Durante o período de implantação e ativação da *PLATAFORMA*, a CONTRATADA deve fornecer apoio à ativação disponibilizando:
     14. Service Desk com atendimento via telefone, e-mail e/ou chat em horário compatível com funcionamento das escolas, regionais e diretorias da CONTRATANTE.
     15. O Suporte deve ser exercido com o objetivo de restabelecer a normalidade de operação e funcionamento mediante saneamento de ocorrências de erros, faltas e falhas decorrentes da implantação, operação e manutenção das soluções de Ensino Remoto definidas pela CONTRATANTE.
     16. As atividades de suporte tecnológico e manutenção corretiva de software deverão ser prestadas pela CONTRATADA:
         1. Ordinariamente, de segunda a sexta feira, no horário comercial;
         2. Extraordinariamente, em circunstância de falta e falha grave da plataforma web e aplicativos que comprometam a prestação dos serviços, em quaisquer dias - inclusive sábados, domingos e feriados – e horários.

As atividades de manutenção corretiva de software e aplicativos, relacionadas ao restabelecimento da normalidade da operação e funcionamento do software serão executados segundo prazos e horários ajustados com o CONTRATANTE na oportunidade de suas respectivas demandas, prazos e horários esses que deverão levar em conta a qualidade, a celeridade e a razoabilidade necessárias às suas respectivas execuções.

**6. REQUISITOS DA CONTRATAÇÃO**

6.1. Toda a *PLATAFORMA* deve atender às normativas de segurança e proteção de dados.

6.2. A *PLATAFORMA* poderá ser similar, superior ou equivalente a exigida, sem violar o Princípio da Isonomia.

* 1. Todo o cronograma de implantação deve ser apresentado as Secretarias Municipais de Educação dos consorciados interessados, com antecedência mínima de 05 (cinco) dias úteis, para análise e aprovação antes do início da implantação.
  2. A execução dos serviços não deve exceder os prazos descritos:
     1. Emissão do “Termo de Subscrição” ou “Licença de Uso” com declaração de emissão das licenças em nome da CONTRATANTE: até 10 (dez) dias após Ordem de Fornecimento das Licenças de Uso.
     2. Entrega dos dispositivos de acesso (chips) contendo a licença de uso para acesso à *PLATAFORMA*: até 60 (sessenta) dias após emissão da Ordem de Fornecimento.
     3. Implantação e Ativação da *PLATAFORMA*: até 60 (sessenta) dias corridos da ordem de fornecimento.
     4. Ativação dos dispositivos: até 30 (trinta) dias corridos após fornecimento dos Dispositivos de Acesso e da Implantação e Ativação da *PLATAFORMA*.
     5. Entrega e disponibilização dos Modens Wi-Fi Portáteis solicitados em até 60 (sessenta) dias após o Ordem de Serviço formalizada e assinada pela CONTRATANTE.
  3. Em relação aos serviços prestados pela CONTRATADA, a mesma deve atender aos prazos de atendimento de acordo com 03 (três) níveis de criticidade:
     1. Alta: Mais de 10% de todos os recursos ou data center inoperante, usuários sem acesso à *PLATAFORMA;*
     2. Média: Menos de 10% dos recursos inoperantes e/ou funções importantes indisponíveis;
     3. Baixa: Situações que afetem apenas usuários específicos/isolados, nunca superando 2% dos usuários ativados com os serviços.
  4. Os serviços incluídos nas Licenças de Uso da *PLATAFORMA* devem ser prestados 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, durante todo o período de vigência do contrato, exceto nos casos de interrupções programadas.
  5. O serviço deve ser realizado de forma ininterrupta, com disponibilidade geral anual mínima em 98% (noventa e oito por cento) do tempo contratado, calculado a partir da média de todos os dispositivos de acesso.
  6. A CONTRATADA deve prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.
  7. Os serviços de Suporte Tecnológicos Presenciais deverão ser prestados em dias úteis e de acordo com os horários de funcionamento (8x5) da CONTRATANTE, e devem ser iniciados em até 15 (quinze) dias a partir da Ordem de Serviço emitida pela CONTRATANTE.
  8. Quanto à locação dos Modens Wi-Fi Portáteis, a CONTRATADA deverá dispor de parque de spare parts equivalente a 3% do total de equipamentos locados pela CONTRATANTE, como forma de atingir a celeridade necessária para atendimento das manutenções demandas pelos usuários e pela fiscalização do contrato.
     1. O Service Desk da CONTRATADA deverá atender as demandas de manutenção dos Modens Wi-Fi Portáteis, abrindo o referido chamado técnico e iniciando o processo de atendimento em conformidade com as melhores práticas previstas nas metodologias ITIL e ITSM.

**7. MODELO DE EXECUÇÃO DO OBJETO**

7.1. A execução seguirá a Ordem de Fornecimento emitida durante a vigência da Ata de Registro de Preços, observando as condições de prestação dos serviços dispostos no ETP e neste Termo de Referência.

1. **CONDIÇÕES E GARANTIA DOS SERVIÇOS**

## A CONTRATADA deverá oferecer garantia contínua da solução durante todo o período de vigência contratual.

## A solução deve ser hospedada durante toda a vigência do contrato em datacenter Tier 3, custeado pela CONTRATADA.

## Os dados da solução devem ser mantidos disponíveis de forma *on-line* durante toda a vigência do contrato.

## Durante o período de vigência do contrato de suporte a CONTRATANTE terá direito a serviços de consultoria especializada na solução contratada.

## Os serviços de consultoria deverão ser prestados pela CONTRATADA e poderão ser usados para atividades como: identificação e mapeamento de processos, elaboração / alteração de painéis, mapeamento de indicadores chave de negócio, elaboração de formulários eletrônicos, estudos de integração entre sistemas, cargas de dados, entre outros.

* 1. Os municípios contratantes poderão exigir, a título de garantia do contrato, e conforme o art. 96, §1° da Lei Federal nº 14.133/2021, o montante de 5 % (cinco por cento) do valor do mesmo, sendo que a pretensa contratada poderá optar por uma das seguintes modalidades:

I - caução em dinheiro ou em títulos da dívida pública emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados por seus valores econômicos, conforme definido pelo Ministério da Economia;

II - seguro-garantia;

III - fiança bancária emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil.

8.3. Para a prestação da garantia pelo contratado quando este optar pela modalidade prevista no item II da cláusula 8.2 o prazo é de 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato.

8.3.1. O prazo de vigência da apólice será igual ou superior ao prazo estabelecido no contrato principal e deverá acompanhar as modificações referentes à vigência deste mediante a emissão do respectivo endosso pela seguradora.

8.3.2. O seguro-garantia continuará em vigor mesmo se o contratado não tiver pago o prêmio nas datas convencionadas.

8.4. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as mesmas condições e coberturas da apólice vigente e desde que nenhum período fique descoberto, ressalvado o disposto no [§ 2º do art. 96 da Lei](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm#art96%C2%A72) n° 14.133/2021.

8.5. A garantia prestada pelo contratado será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, atualizada monetariamente.

**9. MODELO DE GESTÃO DO CONTRATO**

9.1. A execução do objeto será monitorada e fiscalizada pelo órgão ou entidade contratante, com apresentação de relatórios periódicos.

9.2. Matriz de Riscos para Contratação de Serviços Tecnológicos Educacionais:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tipo de Risco** | **Descrição do Risco** | **Probabilidade de Ocorrência** | **Impacto** | **Plano de Mitigação** |
| **Qualidade** | Qualidade dos serviços inferiores, suporte técnico inadequado ou modens WI-FI com desempenho abaixo do esperado | Média | Alto | Realização de testes e avaliações rigorosas antes da contratação, incluindo a exigência de demonstrações. Definição clara de critérios de qualidade no contrato. |
| **Logístico** | Atraso na entrega dos serviços, suporte técnico não atendendo prontamente ou demora na disponibilização dos modens WI-FI | Baixa | Alto | Inclusão de cláusulas contratuais com prazos e penalidades rigorosas para a entrega dos serviços e dos equipamentos. |
| **Financeiro** | Variação nos custos dos serviços, aumento não previsto nos custos do suporte técnico ou modificações nos valores da locação dos modens WI-FI | Alta | Médio | Realização de pesquisa de mercado ampla e detalhada para definição de preços. Estabelecimento de contratos com cláusulas que preveem reajustes apenas em condições específicas e limitam aumentos abruptos. |
| **Jurídico** | Questões legais envolvendo o licenciamento da Plataforma Tecnológica ou problemas contratuais | Média | Alto | Revisão minuciosa dos termos contratuais por profissionais jurídicos especializados. Certificação de conformidade com normas e regulamentações vigentes. |
| **Segurança da Informação** | Vulnerabilidades na segurança da Plataforma Tecnológica ou nos modens WI-FI | Baixa | Muito Alto | Implementação de medidas de segurança robustas e atualizadas. Educação e conscientização dos usuários sobre práticas seguras. |
| **Operacional** | Dificuldades operacionais na implementação da Plataforma Tecnológica ou na utilização dos modens WI-FI | Média | Alto | Realização de treinamentos para usuários e equipe responsável. Estabelecimento de canais de comunicação eficientes para suporte técnico. |
| **Desempenho Educacional** | Falhas na Plataforma Tecnológica afetando negativamente as atividades pedagógicas remotas | Alta | Muito Alto | Desenvolvimento de planos de contingência para situações de emergência. Monitoramento contínuo do desempenho da plataforma. Estabelecimento de canais de comunicação eficientes para reporte de problemas. |

Esta matriz de riscos visa antecipar e gerenciar possíveis desafios que podem surgir ao longo da contratação de serviços tecnológicos educacionais, proporcionando uma abordagem estruturada para mitigação e controle de cada um dos riscos identificados.

**10. CRITÉRIOS DE PAGAMENTO**

10.1. No valor ofertado deverão estar inclusos todos os custos diretos e indiretos, inclusive taxas, impostos, frete e outros que incidam ou venham a incidir na execução do objeto no local estabelecido.

* + 1. Para os itens cuja natureza seja de subscrição (licença de uso), o pagamento será realizado seguindo o cronograma a seguir:
       1. 20% (vinte por cento) do valor do lote encomendado após ateste da fiscalização do contrato e emissão pela CONTRATADA do Termo de Licenciamento de Uso (ou Licença de Uso) constando o nome da contratante, número do contrato, número do empenho, produto licenciado, vigência/prazo da licença de uso, assinatura do representante da CONTRATADA.
       2. 80% (oitenta por cento) do valor após ateste da fiscalização do contrato acerca do recebimento físico dos Chips/Dispositivos de Acesso que contém a licença de uso instalada para viabilizar o acesso à *PLATAFORMA*, com validade e vigência de 12 (doze) meses após a data de ativação do serviço.
    2. Para os itens cuja natureza seja de subscrição (licença de uso), a Nota Fiscal de Serviços a ser emitida pela CONTRATADA deverá prever a correta classificação do serviço relacionado a Licença de Uso de Software relacionada a Processamento remoto de dados em ambiente remoto de infraestrutura de TI (Data Center ou Centro de Processamento de Dados). Nestes itens, dada a natureza do serviço de processamento remoto dos dados, não incidirá retenção do ISS na localidade da CONTRATANTE;
    3. Para o item de LOCAÇÃO do equipamento Modem Wi-Fi Portátil, a CONTRATADA deverá apresentar mensalmente um Boletim de Medição contendo o relatório com a lista dos equipamentos locados, bem como o valor pró-rata dia para aqueles itens que forem entregues ao longo do mês de apuração. As faturas deverão ser acompanhadas de Recibo de Locação de Equipamentos Móveis, e estarão isentas de recolhimento de ISS municipal (Imposto Sobre Serviços), conforme legislação federal para locação de equipamentos móveis. A fiscalização do contrato irá avaliar, solicitar correção e atestar mensalmente o Boletim de Medição considerado correto.
    4. Para os itens de Prestação de Serviços de Suporte Tecnológico, a CONTRATADA deverá emitir Nota Fiscal de Serviços, registrando a retenção do ISS no destino (local da CONTRATANTE).

**11. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR**

11.1. A seleção do fornecedor ocorrerá por meio de processo licitatório, de acordo com a legislação vigente, modalidade pregão eletrônico, conforme previsto na Lei Federal n° 14.133/2021.

11.1.1. A seleção levará em consideração o MENOR PREÇO POR LOTE, de acordo com as condições, quantidades e exigências estabelecidas.

# Habilitação/Qualificação Técnica:

11.2.1 A CONTRATANTE deverá apresentar atestado(s) fornecido por pessoa(s) jurídica(s) de direito público ou privado, comprovando que desempenhou atividade pertinente e compatível em características, quantidades e prazos com o objeto desta licitação. Para efeito de comprovação da capacidade técnica da licitante, as parcelas de maior relevância são:

* A licitante deverá apresentar junto aos Documentos de Habilitação a documentação técnica da *PLATAFORMA* e Modem Wi-Fi Portátil ofertada que permita à Contratante verificar o atendimento aos requisitos técnicos contidos no ETP e neste Termo de Referência.
* Desenvolvimento e disponibilização de aplicativos (softwares) customizados para ambiente WEB e Mobile, hospedados em data center com infraestrutura de TIC de alta disponibilidade;
* Prestação de serviços contínuos de processamento/conectividade/transmissão de dados via redes de comunicação móvel GSM/GPRS para dispositivos eletrônicos móveis com funcionalidades de controle e gestão sobre os acessos dos dispositivos e troca remota do provedor de acesso à Internet: mínimo de 5.000 (cinco mil) equipamentos/dispositivos simultâneos, por um período mínimo de 12 (doze) meses;
* Locação de equipamentos eletrônicos, incluindo serviços de suporte técnico remoto e manutenção em campo: mínimo de 500 (quinhentos) equipamentos, por um período mínimo de 12 (doze) meses;
* Implantação e manutenção por, no mínimo, 12 (doze meses) de solução de segurança da informação (Firewall) e ferramentas de filtro de conteúdo, para ambientes de infraestrutura de TIC de alta disponibilidade;
* Prestação de serviços de atendimento aos usuários em 1º e 2º Nível, na modalidade Service Desk, de forma remota e presencial, englobando operação continuada de uma Central de Serviços, assistência técnica a hardwares e suporte de softwares (desktops, notebooks, impressoras ou dispositivos eletrônicos portáteis) em parque com, pelo menos, 1.000 (hum mil) equipamentos.

11.2.2. No caso de atestado fornecido a consórcio do qual o licitante tenha participado, só será aceito se o mesmo tiver executado totalmente ou parcialmente os serviços, que servirão de comprovação da aptidão técnica exigida no edital. Os atestados podem ser complementados por descritivos mais detalhados elaborados pelo contratante (cliente) da licitante, devidamente assinado por pessoa identificada e oficialmente vinculada ao emissor do Atestado.

# Amostra/Laudo Técnico/Prova de Conceito

## A documentação técnica apresentada pela Licitante deve ser composta por catálogos ou datasheets elaborados pelos fabricantes dos componentes mais relevantes da *PLATAFORMA* ofertada e indicar os modelos ou part numbers de tais componentes, a saber:

## A licitante deve apresentar, no mínimo, catálogos e datasheets dos seguintes componentes:

## Dispositivo de Acesso (chip)

## Solução de Firewall

## Solução de Balanceamento de Carga

## Data Center Tier III

## Modem Wi-Fi Portátil

## A sessão para realização da Prova de Conceito junto ao licitante provisoriamente classificado em primeiro lugar será agendada pelo(a) pregoeiro(a) após avaliação e aprovação da documentação de habilitação da licitante arrematante, em conformidade com os prazos definidos neste Edital e seus anexos, e a comunicação se dará por meio de correio eletrônico para todos os representantes legais das licitantes, onde constarão a data, hora e local da realização da sessão de Prova de Conceito. As licitantes que optarem por acompanhar presencialmente a sessão da Prova de Conceito poderão indicar 01 (hum) representante para esta etapa.

## Caso as soluções apresentadas pelo Licitante possuam mais de um componente para pleno atendimento das especificações do ANEXO I ele deverá apresentar todos os documentos (catálogos e datasheets) de todos os componentes que comprovem o atendimento de todos os itens técnicos da *PLATAFORMA*.

## A LICITANTE provisoriamente colocada em primeiro lugar será convocada pela Pregoeira a participar de teste de homologação da solução proposta, nos moldes descritos no item 10.15 e seguintes.

## A CONTRATANTE exigirá um teste de prova de conceito da *PLATAFORMA* proposta, que consiste na comprovação pela Licitante da disponibilidade imediata dos recursos essenciais e indispensáveis dentre aqueles descritos nas especificações do ANEXO I, por meio da etapa de realização de testes práticos em bancada. Os requisitos exigidos na Prova de Conceito estão descritos com clareza e objetividade no item 10.15 e seguintes deste Termo de Referência.

## Como forma de receber aprovação em determinado teste, não serão aceitas promessas de execução das funcionalidades, mesmo que estas possuam data definida, dado que estes tipos de documentos não exprimem garantia de que a LICITANTE possui capacidade técnica para cumprir os requisitos previstos no Edital e ANEXOS estritamente necessários para o funcionamento e a segurança da solução durante a vigência do contrato e dentro dos prazos definidos pela CONTRATANTE neste documento.

## Ambiente de Teste:

## A LICITANTE mais bem classificada na etapa de disputa de preços será convocada para, em até 5 (cinco) dias úteis, participar de reunião inaugural presencial na CONTRATANTE para discussões relativas à execução dos testes de homologação da solução. Essa reunião tem a finalidade de apresentar, ao LICITANTE classificado em primeiro lugar, o ambiente físico onde serão executados os testes e dirimir eventuais dúvidas do LICITANTE sobre a forma de execução da prova de conceito. A reunião será agendada pela Pregoeira.

## No dia imediatamente posterior à reunião inaugural começa a contagem do prazo máximo de 05 (cinco) dias úteis para a LICITANTE apresentar, instalar e configurar as amostras para execução do teste de aceitação da *PLATAFORMA* e do Modem Wi-Fi Portátil pela CONTRATANTE.

## As atividades realizadas pela LICITANTE ficarão restritas ao horário de expediente da CONTRATANTE.

## As amostras a serem fornecidas e os testes que deverão ser realizados encontram-se previstos e firmemente definidos no ANEXO II deste Termo de Referência.

## A LICITANTE ficará condicionada a utilizar os mesmos equipamentos e softwares apresentados no ambiente de testes, durante toda execução do contrato com a Secretaria de Educação.

## Outras hipóteses de substituição dos modelos e marcas dos equipamentos ofertados deverão ser apresentadas à CONTRATANTE, que analisará a possibilidade de permuta dos itens, desde que comprovado o atendimento completo aos requisitos previstos nas especificações deste Termo de Referência.

## A LICITANTE deve apresentar ao menos um profissional, com conhecimento da *PLATAFORMA* e dos componentes ofertados, para acompanhar e orientar a avaliação da solução.

## As amostras serão examinadas e avaliadas pelos servidores do Departamento de TI da CONTRATANTE, que terão o prazo de até 05 (cinco) dias úteis para emissão do parecer técnico sobre a aprovação (ou não) da amostra apresentada.

## O prazo acima poderá ser excepcionalmente prorrogado, a critério do CIM-JEQUITINHONHA, por até 3 (três) dias úteis, visando a permitir a realização de testes mais detalhados que a equipe técnica entender necessários.

## Para eventual participação no Ambiente de Testes os demais participantes do certame tomarão ciência da data, local e hora de realização dos procedimentos do ambiente de testes.

## Durante a etapa de apresentação da amostra pela LICITANTE convocada, os demais participantes não poderão interferir ou prejudicar a realização dos testes. Quaisquer manifestações desejadas pelas demais licitantes deverão ser formalizadas por meio de documento formal assinado pelo representante legal da LICITANTE em prazo de até 02 (dois) dias úteis após a conclusão da apresentação da amostra.

* 1. Todas as despesas e providências decorrentes da apresentação da amostra, tais como, mão de obra, transporte, seguro, emissão de laudos, bem como quaisquer outras de ordem material, que se fizerem necessárias ao cumprimento do edital, são de responsabilidade da LICITANTE, não cabendo qualquer ônus ao CIM-JEQUITINHONHA.
  2. A recusa em providenciar os testes, bem como a não aceitação justificada da *PLATAFORMA* pelo CIM-JEQUITINHONHA, mediante relatório técnico, acarretará a desclassificação da LICITANTE.
  3. O Pregoeiro(a) informará a data e a hora em que será divulgado o resultado da etapa de avaliação da amostra e será dado prosseguimento às demais sessões do pregão.
  4. Será emitido um relatório descrevendo os testes realizados e contendo a aprovação ou não da amostra apresentada.
  5. Em caso de desclassificação da LICITANTE, os equipamentos utilizados deverão ser recolhidos em até 5 (cinco) dias úteis contados da divulgação da desclassificação.

10.15. A Licitante classificada provisoriamente como arrematante da disputa de preços deverá apresentar amostra da *PLATAFORMA* a ser fornecida e do Modem Wi-Fi Portátil a ser locado, de forma que a Contratante possa certificar a capacidade técnica de fornecimento do objeto licitado.

10.15.1. A apresentação da Amostra pela licitante melhor classificada será realizada em sessão presencial agendada especificamente para esta finalidade, nas dependências da Contratante, em prazo máximo de 05 (cinco) dias úteis após a declaração da empresa arrematante da disputa de preços.

10.15.2. A apresentação da Amostra poderá ser acompanhada por até 02 (dois) representantes das demais licitantes, deverá durar até 08 (oito) horas e cumprir a sequência abaixo definida:

|  |  |  |
| --- | --- | --- |
| Critério a ser Avaliado | Atendimento às especificações | Justificativas |
| Documentação técnica da *PLATAFORMA* e do MODEM WI-FI PORTÁTIL apresentada permite verificar o atendimento aos requisitos técnicos exigidos no Termo de Referência. | ( ) Atendeu  ( ) Não atendeu |  |
| A Licitante deverá apresentar um Equipamento Móvel comum no mercado (Smartphone ou Tablet com sistema operacional Android) utilizando um Dispositivo de Acesso à *PLATAFORMA* proposta funcionando, porém, com a navegação Internet via browser totalmente bloqueada.  A Licitante deverá disponibilizar ferramenta WEB ou APP para que a equipe da Contratante possa abrir um chamado técnico solicitando a liberação de uma URL específica e de conhecimento público (definida no exato momento do teste pela Contratante).  A Licitante deverá proceder o cadastro desta URL solicitada na sua *PLATAFORMA*, de forma que o usuário do mesmo Dispositivo Móvel utilizado passe a conseguir acessar o conteúdo da URL em questão via browser do Dispositivo Móvel utilizado. | ( ) Atendeu  ( ) Não atendeu |  |
| A Licitante deverá disponibilizar ferramenta WEB ou APP para que a equipe da Contratante possa abrir um chamado técnico solicitando a troca/substituição remota do provedor de conectividade ou operadora de telefonia móvel previamente configurada no Dispositivo de Acesso da *PLATAFORMA*, sem a necessidade de substituição física no local de componentes previamente instalados no Tablet ou Smartphone.  A licitante poderá utilizar na demonstração desta funcionalidade qualquer Dispositivo Móvel (smartphone ou tablet) que permita apresentar a efetividade do remoto para troca/substituição remota do provedor de conectividade ou operadora de telefonia móvel. | ( ) Atendeu  ( ) Não atendeu |  |
| A Licitante deverá disponibilizar MODEM WI-FI PORTÁTIL, carregado com o referido Dispositivo de Acesso à Plataforma oferecido, com alimentação proveniente da bateria interna do equipamento, em funcionamento.  O Modem deverá disponibilizar uma rede Wi-Fi para conexão segura com senha de equipamentos diversos (notebooks ou smartphones) e disponibilização de conexão à Internet de endereços web (url) liberados (whitelist) na PLATAFORMA ofertada.  Endereços web (url) não liberados (blacklist) deverão estar bloqueados e não devem ser acessados pelos equipamentos conectados nesta rede Wi-Fi. | ( ) Atendeu  ( ) Não atendeu |  |
| Licitante atendeu todos os requisitos: | ( ) Atendeu  ( ) Não atendeu |  |

**12. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO**

12.1. As estimativas de valores, memórias de cálculo e documentos correlatos foram elaborados em documento à parte e classificados adequadamente, conforme consta anexo ao processo de contratação.

**13. ADEQUAÇÃO ORÇAMENTÁRIA**

13.1. A contratação deverá estar em consonância com o orçamento disponível para o exercício financeiro de cada órgão contratante.

O presente Termo de Referência foi elaborado em estrita conformidade com a Lei Federal nº 14.133/2021, seus anexos e alterações, bem como com outros dispositivos legais pertinentes.

Diamantina/MG, 05 de abril de 2024

**Lilia Fagundes Trindade Nascimento**

**Coordenadora Administrativa do CIM JEQUITINHONHA**

Anexo I ao Termo de Referência

**REQUISITOS DA PLATAFORMA DE GESTÃO E CONTROLE DOS ACESSOS E CONECTIVIDADE**

A Plataforma de Gestão e Controle dos Acessos e Conectividade (*PLATAFORMA*) fornecida na modalidade PaaS (*Plataform as a Service*) pela CONTRATADA deve possuir capacidade para processar todos os dispositivos de acesso simultaneamente, o que representa 100% dos usuários conectados simultaneamente aos servidores de conteúdo disponibilizados pela Secretarias Municipais de Educação para a educação remota.

A *PLATAFORMA* deve atender integralmente os seguintes requisitos e funcionalidades:

1. Ter a capacidade de gerenciar os eUICCs através de plataforma eSIM Management compatíveis com a especificação GSMA SGP.02 v3.2.
2. Possuir capacidade de gerenciamento fim a fim, possuindo SM-DP e SM-SR e fornecimento dos chips eUICCs.
3. Plataforma hospedada em pelo menos 2 DataCenters certificados GSMA SAS-SM Accredited Sites em diferentes continentes, incluindo Ásia e América.
4. Possuir capacidade de interoperabilidade com diferentes fabricantes de dispositivos e eSIM cards.
5. Para atender a todas as necessidades e funcionalidades apontadas no Termo de Referência e respeitar a Lei Geral de Proteção de Dados a plataforma deve possuir no mínimo as soluções abaixo:

* Solução de Firewall de Próxima Geração
* Solução de Balanceamento de Carga
* Solução de Armazenamento de Logs e Relatórios.

As especificações mínimas de cada solução são descritas abaixo:

* 1. **Solução de Firewall**
  2. A Solução de Firewall instalado no Data Center da CONTRATADA deve ser composto por hardware e software.
  3. A Solução de Firewall deve monitorar o tráfego de rede de entrada e saída e decidir permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.
  4. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração.
  5. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
  6. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.
  7. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada
  8. A Solução de Firewall deve possuir no mínimo as seguintes características:
     1. Throughput de, no mínimo, 140 Gbps com a funcionalidade de firewall habilitada, independentemente do tamanho do pacote.
     2. Suporte a, no mínimo, 12.000.000 conexões simultâneas.
     3. Suporte a, no mínimo, 700.000 novas conexões por segundo.
     4. Throughput de, no mínimo, 50 Gbps de VPN IPSec.
     5. Deve estar licenciado para, ou suportar sem o uso de licença, 15.000 túneis de VPN IPSEC Site-to-Site simultâneos.
     6. Deve estar licenciado para, ou suportar sem o uso de licença, 80.000 túneis de clientes VPN IPSEC simultâneos.
     7. Throughput de, no mínimo, 10 Gbps de VPN SSL.
     8. Suporte a, no mínimo, 5000 clientes de VPN SSL simultâneos.
     9. Suportar no mínimo 12 Gbps de throughput de IPS.
     10. Suporte a, no mínimo, 30 Gbps de throughput de Application Control.
     11. Suportar no mínimo 15 Gbps de throughput de Inspeção SSL.
     12. Throughput de, no mínimo 9 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware.
     13. Caso o fabricante escolhido pela CONTRATADA divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.
     14. Deve possuir ao menos 2 interfaces 10 GE SFP+.
     15. Deve possuir ao menos 16 interfaces 1 GE RJ-45.
     16. Deve possuir ao menos 8 interfaces 1 GE SFP.
     17. Deve possuir ao menos 12 interfaces 25GE SFP28.
     18. Deve possuir ao memos 4 interfaces 40GE QSFP+.
     19. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance.
  9. O equipamento de firewall deve possuir alimentação Dual / tensão de 100-240 VAC.
  10. O equipamento de firewall deve possuir alimentação Dual / frequência de 50/60 Hz.
  11. O equipamento de firewall deve possuir deve possuir fonte de alimentação redundante que permitam troca a quente e caso de defeito.
  12. O equipamento de firewall deve possuir temperatura - faixa de operação de 0º a 40º C.
  13. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.
  14. Os dispositivos de proteção de rede devem possuir:
      1. suporte a 4094 VLAN Tags 802.1q.
      2. suporte a Policy based routing ou policy based forwarding.
      3. suporte a roteamento multicast (PIM-SM e PIM-DM).
      4. suporte a DHCP Relay.
      5. suporte a DHCP Server.
      6. suporte a Jumbo Frames.
  15. Os dispositivos de proteção de rede devem suportar:
      1. sub-interfaces ethernet logicas.
      2. NAT dinâmico (Many-to-Many).
      3. NAT estático (1-to-1).
      4. NAT estático bidirecional 1-to-1.
      5. Tradução de porta (PAT).
      6. NAT de Origem.
      7. NAT de Destino.
      8. NAT de Origem e NAT de Destino simultaneamente.
  16. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
  17. Deve suportar NAT64 e NAT46.
  18. Deve implementar o protocolo ECMP.
  19. Deve implementar balanceamento de link por hash do IP de origem.
  20. Deve implementar balanceamento de link por hash do IP de origem e destino.
  21. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links.
  22. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais.
  23. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação.
  24. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo e twamp.
  25. Deve permitir a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo.
  26. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação.
  27. A solução deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência).
  28. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas.
  29. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de roteamento.
  30. Deve permitir monitorar via SNMP falhas de hardware, monitoramento de CPU e memória, de segurança e interface.
  31. Deve enviar log para sistemas de monitoração externos, simultaneamente.
  32. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL.
  33. Deve possuir proteção anti-spoofing.
  34. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).
  35. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).
  36. Deve suportar OSPF graceful restart.
  37. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.
  38. Deve suportar Modo Camada 2 (L2), para inspeção de dados em linha e visibilidade do tráfego.
  39. Deve suportar Modo Camada 3 (L3), para inspeção de dados em linha visibilidade do tráfego.
  40. Deve suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente.
  41. Deve suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3.
  42. Deve suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster.
  43. Deve realizar configuração em alta disponibilidade deve sincronizar: Sessões.
  44. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede.
  45. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs.
  46. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB.
  47. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
  48. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance.
  49. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos.
  50. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas.
  51. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos).
  52. Controle por Política de Firewall.
  53. Deve suportar controles por zona de segurança.
  54. Deve possuir controles de políticas por porta e protocolo.
  55. Deve possuir controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
  56. Deve possuir controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
  57. Deve possuir controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).
  58. Deve possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
  59. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound).
  60. Deve descriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2.
  61. Deve possuir controle de inspeção e descriptografia de SSH por política.
  62. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada.
  63. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo).
  64. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
  65. Deve ter suporte a objetos e regras IPV6.
  66. Deve ter suporte a objetos e regras multicast.
  67. Deve suportar no mínimo dois tipos de resposta nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão.
  68. Deve suportar atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
  69. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.
  70. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
  71. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.
  72. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs.
  73. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.
  74. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor.
  75. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.
  76. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex.
  77. Deve identificar o uso de táticas evasivas via comunicações criptografadas.
  78. Atualizar a base de assinaturas de aplicações automaticamente.
  79. Deve permitir a limitação da banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos.
  80. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.
  81. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.
  82. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.
  83. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.
  84. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante.
  85. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL.
  86. A solução utilizada pela CONTRATADA deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.
  87. Deve alertar o usuário quando uma aplicação for bloqueada.
  88. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc.) possuindo granularidade de controle/políticas para os mesmos.
  89. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos.
  90. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo.
  91. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos.
  92. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc.).
  93. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação.
  94. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.
  95. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall.
  96. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).
  97. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.
  98. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade.
  99. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset.
  100. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.
  101. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.
  102. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.
  103. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
  104. Deve permitir o bloqueio de vulnerabilidades.
  105. Deve permitir o bloqueio de exploits conhecidos.
  106. Deve incluir proteção contra-ataques de negação de serviços.
  107. Deve possuir o seguinte mecanismo de inspeção de IPS:
       1. Análise de padrões de estado de conexões.
       2. Análise de decodificação de protocolo.
       3. Análise para detecção de anomalias de protocolo.
       4. Análise heurística.
       5. IP Defragmentation.
       6. Remontagem de pacotes de TCP.
       7. Bloqueio de pacotes mal formados.
  108. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.
  109. Deve detectar e bloquear a origem de portscans.
  110. Deve bloquear ataques efetuados por worms conhecidos.
  111. Deve possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.
  112. Deve possuir assinaturas para bloqueio de ataques de buffer overflow.
  113. Deve possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.
  114. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações.
  115. Deve permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.
  116. Deve identificar e bloquear comunicação com botnets.
  117. Deve registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.
  118. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou por filtro pré-definido.
  119. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.
  120. Os eventos devem identificar o país de onde partiu a ameaça.
  121. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
  122. Deve possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
  123. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc., ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
  124. Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).
  125. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.
  126. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local.
  127. Deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.
  128. Deve possuir pelo menos 60 categorias de URLs.
  129. Deve possuir a função de exclusão de URLs do bloqueio, por categoria.
  130. Deve permitir a customização de página de bloqueio.
  131. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site).
  132. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local.
  133. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.
  134. Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2.
  135. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc.
  136. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
  137. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.
  138. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).
  139. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.
  140. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.
  141. Deve permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução.
  142. Deve prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.
  143. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se 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.
  144. Deve suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem.
  145. Deve suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino.
  146. Deve suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo.
  147. Deve suportar a criação de políticas de QoS e Traffic Shaping por aplicações.
  148. Deve suportar a criação de políticas de QoS e Traffic Shaping por porta.
  149. O QoS deve possibilitar a definição de tráfego com banda garantida.
  150. O QoS deve possibilitar a definição de tráfego com banda máxima.
  151. O QoS deve possibilitar a definição de fila de prioridade.
  152. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
  153. Suportar marcação de pacotes Diffserv, inclusive por aplicação.
  154. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping.
  155. Deve suportar identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc.) identificados sobre aplicações (HTTP, FTP, SMTP, etc.).
  156. Deve suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos.
  157. Deve suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.
  158. Deve 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.
  159. Deve suportar a criação de políticas por geolocalização, permitindo o trafego de determinado Pais/Países sejam bloqueados.
  160. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
  161. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.
  162. Deve suportar VPN Site-to-Site e Cliente-To-Site.
  163. Deve suportar IPSec VPN.
  164. Deve suportar SSL VPN.
  165. A VPN IPSEc deve suportar 3DES.
  166. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.
  167. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.
  168. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).
  169. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard).
  170. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.
  171. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
  172. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting.
  173. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.
  174. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.
  175. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies.
  176. Atribuição de DNS nos clientes remotos de VPN.
  177. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.
  178. Deve suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local.
  179. Deve suportar leitura e verificação de CRL (certificate revocation list).
  180. Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.
  181. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação.
  182. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação.
  183. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário.
  184. Deverá manter uma conexão segura com o portal durante a sessão;
  185. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior).
  186. Durante a vigência do contrato a CONTRATADA deve manter os softwares sempre atualizados na versão mais recente sem nenhum custo adicional.

1. **Solução de Balanceamento de Carga**
   1. Devido a grande quantidade de acessos simultâneos na plataforma a CONTRATADA deve possuir dentro da solução e Data Center Tier III ou similar sistema de balanceamento de carga com as seguintes características:
      1. Throughput mínimo de camada 4 de 40 Gbps.
      2. Throughput mínimo de camada 7 de 25 Gbps.
      3. Deve suportar no mínimo 35 milhões de conexões concorrentes.
      4. Deve possuir aceleração de SSL baseada em hardware.
      5. Deve estar licenciado para no mínimo 30 instâncias virtuais.
      6. Deve possuir ao menos 128 GB de disco.
      7. Deve possuir ao menos 6 interfaces gigabit ethernet RJ-45.
      8. Deve possuir ao menos 6 interfaces gigabit ethernet SFP.
      9. Deve possuir ao menos 4 interfaces 10 gigabit ethernet.
   2. Deve suportar a criação de contas de administradores com diferentes perfis de acesso e direitos (Role based).
   3. A solução deve permitir balancear em camada 7 os seguintes protocolos: HTTP, HTTPs, TurboHTTPS, RADIUS, RDP, SIP, TCPs, DNS, SMTP, RTMP, RTSP, MySQL.
   4. Deve balancear tráfego entre servidores reais usando algoritmos próprios e usado informação de saúde de servidores reais.
   5. Deve permitir a configuração de perfis que determinem a criptografia do tráfego entre o equipamento e os servidores reais.
   6. Quando houver comunicação encriptada esta deverá ser controlada por protocolos SSL/TLS e lista de ciphers.
   7. Deve suportar os protocolos SSL (v2 e v3) e TLS (v1.0, v1.1, v1.2).
   8. Deve suportar ao menos os seguintes ciphers: ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA384, AES256-GCM-SHA384, AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, AES128-SHA, RC4-SHA.
   9. Deve ser capaz de reutilizar sessões SSL.
   10. Para cada um dos servidores que participarão do algoritmo de balanceamento deve ser possível configurar: peso (para fins de controle de preferência de encaminhamento de tráfego), o número máximo de conexões suportadas por aquele servidor, o limite máximo de novas conexões por segundo que aquele servidor suporta, diferentes métodos de verificação de saúde, perfil de encriptação entre o sistema e este servidor (SSL/TLS e cipher) e configuração de atraso para encaminhamento de conexões ao servidor caso este tenha sido reiniciado, taxa máxima de novas conexões durante o intervalo de tempo seguinte a reinicialização do servidor, cookie (para fins de identificação de conexões) e indicação se este servidor é backup de outro(s).
   11. O equipamento oferecido deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos: endereço de origem, hash de endereço de origem, hash que inclui endereço e porta TCP/UDP, hash baseado em cookie provido pelo servidor real, identificação de sessão SSL, hash de um palavra específica encontrada no cabeçalho de requisição HTTP do cliente, hash de parâmetro de URL encontrado em requisição HTTP vinda do cliente, atributo de RADIUS.
   12. Deve ter capacidade de reescrever o cookie vindo do servidor real para uso em regras de persistência.
   13. Deve suportar a configuração de timeouts de conexão submetidas a persistência.
   14. O sistema deve permitir a seleção do servidor real baseado em informação de cabeçalho de pacotes TCP/IP e HTTP.
   15. Deve possibilitar a seleção de servidor real baseado em valor de campos de cabeçalho HTTP incluindo pelo menos os conteúdos de HTTP Host, HTTP Referer, HTTP Request URL e SNI (server Name Indicator).
   16. A seleção por campos de cabeçalho HTTP para fins de roteamento deverá ser feita através de expressões regulares ou match completo.
   17. O sistema deve permitir a reescrita de mensagens de HTTP request, HTTP Response e de cabeçalho HTTP.
   18. O sistema deve possibilitar reescrita do parâmetro Location de resposta HTTP condicionado ao uso de strings ou expressões regulares para identificar padrões sobre os campos: HTTP host, HTTP location, HTTP Referer, HTTP Request URL e endereço de IP de origem.
   19. O sistema deve possibilitar reescrita, redirecionamento, ou proibir requests HTTP. Deve possibilitar a reescrita dos parâmetros host, URL e Referer do cabeçalho HTTP. Estas operações devem estar condicionadas ao uso de strings ou expressões regulares para identificar padrões sobre os campos: HTTP host, HTTP location, HTTP Referer, HTTP Request URL e endereço de IP de origem.
   20. O sistema deve possibilitar compressão de dados incluindo: aplicações (java script, SOAP XML, X-javascript, XML) e Texto (CSS, HTML, JavaScript, Plain, XML).
   21. O sistema deve implementar cache de conteúdo para HTTP, permitindo que objetos sejam armazenados em memória e requisições HTTP sejam respondidas diretamente pela solução, e que este cache:
       1. Para fins de controle de uso de recursos deve ser possível controlar: tamanho máximo de objeto, tamanho máximo de cache do sistema, número máximo de entradas de cache, tempo máximo de cache, regras de exceção.
   22. O sistema deve possuir perfis de tráfego pre configurados para uso em grupo de servidores reais. Pelo menos os seguintes perfis de serviços/servidores devem estar pre configurados: FTP, TCP, UDP, HTTP Seguro (com offload de TLS/SSL), RADIUS, TCP Seguro (com offload de TLS/SSL).
   23. Além dos perfis pré-configurados o sistema deve permitir a customização dos perfis baseado em bloqueio ou permissão de endereço IP de origem baseado na localização por país (TCP, UDP, HTTP, FTP, HTTP), reputação de endereço de origem (TCP, UDP, HTTP, FTP, HTTP) mantida pelo fabricante, compressão de dados (HTTP), cache de dados (HTTP).
   24. O sistema deve permitir a personalização de páginas de erro enviadas aos clientes em caso de falha nos servidores. Estas páginas devem ser editadas em HTML;
   25. Deve implementar NAT, NAT64 e NAT46 (os dois últimos para permitir NAT incluindo IPv4 e IPv6 entre clientes e servidores).
   26. Deve implementar esquema de autenticação Basic (RFC 2617).
   27. Deve ter algoritmos de balanceamento de carga pré configurados incluindo pelo menos: Round Robin (seleciona o próximo servidor de uma série pré-configurada), seleção do servidor com menor número de conexões correntes, servidor com a melhor ´saúde´, seleção baseada no hash da URI (cabeçalho HTTP), seleção baseada no hostname (HTTP request), seleção baseada no hash do endereço IP de destino.
   28. Deve possuir mecanismos de balanceamento de tráfego através de vários enlaces de comunicação.
   29. Deve possibilitar o balanceamento de tráfego inbound (da WAN para a LAN) e outbound (de LAN para a WAN) usando múltiplos enlaces WAN.
   30. O tráfego a ser balanceado deve ser selecionado através: de endereços (ou grupo de endereços) IP de origem e de destino, serviços TCP ou UDP, em função do horário (hora, dia, mês, ano), e blocos de endereços de Internet Service Providers.
   31. Deve possuir mecanismos de persistência de tráfego que ignore algoritmos de balanceamento de tráfego.
   32. Os mecanismos de persistência devem ser estabelecidos em função de endereços IP destino e origem.
   33. Deve possuir mecanismos de seleção de rotas em função de latência de tráfego ao destino medido através de ICMP ou TCP echo.
   34. Para um dado grupo de enlaces de comunicação usados para balanceamento de tráfego, os algoritmos de distribuição de tráfego devem fazer uso de, pelo menos, os seguintes parâmetros: número de conexões sendo tratadas pelo enlace, taxa de novas conexões sendo abertas no enlace, menor quantidade de tráfego entrante do enlace, menor quantidade de tráfego sainte do enlace, soma de tráfego entrante e sainte do enlace, utilização de enlaces (entrada e saída) ou peso dado ao enlace.
   35. Deve ser capaz de estabelecer túneis virtuais com sistemas do mesmo fabricante para transporte de tráfego entre os equipamentos.
   36. Suporte a estabelecimento de túneis usando encapsulamento GRE (Generic Routing Encapsulation).
   37. Deve balancear o tráfego entre estes enlaces virtuais baseado em pesos atribuídos aos enlaces ou função de cálculos de hash de endereços IP de origem e destino.
   38. Suporte a monitoramento de estado de saúde de links com ISPs e enlaces virtuais.
   39. Deve ser possível estabelecer um dos enlaces (virtual ou real) como enlace de backup (usado somente quando primários não estão disponíveis).
   40. As interfaces de rede devem suportar protocolo Ethernet com pelo menos as seguintes velocidades: 10 Mbps (half e full duplex), 100 Mbps (half e full duplex), 1000 Mbps (half e full duplex) e autonegociação.
   41. Deve implementar o protocolo IEEE 802.3ad para balanceamento de tráfego entre portas.
   42. Deve implementar VLANs e ser compatível com o protocolo IEEE 802.1q.
   43. Deve permitir o roteamento entre diferentes VLANs.
   44. Deve suportar a configuração de rotas estáticas incluindo a distância administrativa da mesma para fins de decisão de roteamento de pacotes.
   45. Deve oferecer suporte a políticas de roteamento baseado em endereços IP de origem e/ou destino.
   46. Deve suportar OSPF v2 - RFC 2328.
   47. Deve implementar NAT (Network Address Translation) incluindo as seguintes modalidades: Source NAT (mudança do endereço IP de origem), mapeamento 1-1 e encaminhamento de portas (UDP ou TCP).
   48. Deve fazer alocação de banda passante baseado no trio endereço destino, endereço de origem e serviço (portas TCP e UDP).
   49. O equipamento oferecido deverá ser capaz de abrir um número reduzido de conexões TCP com o servidor e inserir os pacotes gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço.
   50. Deve implementar cache de caminho reverso assegurando que a resposta a um cliente seja encaminhada através do mesmo provedor usado no recebimento de pacote do mesmo.
   51. Deve suportar implementação em modo transparente, atuando como Bridge L2.
   52. Deve implementar mecanismos de verificação de ´saúde´ em serviços remotos através de, pelo menos, os seguintes protocolos: ICMP, TCP Echo, TCP, HTTP, HTTPS, DNS, RADIUS, SMTP, POP3, IMAP4, RADIUS Accounting, FTP, TCP Half Open, TCP SSL, SNMP, SSH, L2 Detection, UDP, ARP e NDP (IPv6).
   53. Deve possuir funcionalidades de Global Server Load Balancing.
   54. Deve implementar servidor DNS baseado em versão protegida de BIND versão 9.
   55. Deve implementar servidor DNS Autoritativo.
   56. Deve permitir o balanceamento de tráfego entre diversos sítios remotos baseado em DNS e tendo como parâmetros, pelo menos, localização, ´saúde´ de servidores e tempo de resposta de aplicações em ambos IPv4 e IPv6.
   57. Deve suportar DNSSEC com algoritmo RSASHA1.
   58. Deve implementar DNS64 para permitir comunicação entre client IPv4 com servidores IPv6 no escopo de balanceamento de carga global.
   59. Deve possibilitar estabelecer a configuração de sítios baseados em localização geográfica (países) e, para caso da China em províncias e provedores de acesso Internet. A base de dados associando endereços IP a países deve ser desenvolvida e gerenciada pelo fabricante.
   60. Deve implementar mecanismos de verificação de ´saúde´ em serviços remotos através de, pelo menos, os seguintes protocolos: ICMP, TCP Echo, TCP, HTTP, HTTPS, DNS, RADIUS, SMTP, POP3, IMAP4, RADIUS Accounting, FTP, TCP Half Open, TCP SSL, SNMP, SSH, L2 Detection, UDP, ARP e NDP (IPv6).
   61. Deve possibilitar a definição de disponibilidade de serviços através de verificação de saúde em vários protocolos baseados em expressões com AND e OR.
   62. Suportar a criação de políticas de DNS. Entende-se por políticas de DNS a maneira pela qual o balanceador irá interpretar e responder a uma requisição DNS, levando em conta os seguintes parâmetros: proximidade geográfica, proximidade de tempo e algoritmo de distribuição de pedidos.
   63. A implementação do mecanismo de proximidade geográfica deve levar em conta o endereço de IP de origem (país) e endereço de destino (país). A associação entre endereços IP e países deve ser implementada e gerenciada pelo fabricante e incluída no sistema.
   64. A implementação do mecanismo de proximidade de tempo deve ser baseada em ICMP e/ou TCP.
   65. Para cada um dos possíveis sítios remotos deve ser possível atribuir peso aos mesmos para que este parâmetro seja levado em conta na sequência de distribuição de respostas DNS.
   66. Quando implementado como servidor DNS autoritativo deve permitir a configuração de número máximo de respostas fornecidas por segundo.
   67. Deve permitir a troca de portas HTTP, HTTPS, Telnet e SSH para fins de acesso remoto ao equipamento por parte do administrador.
   68. Deve suportar a sincronização de horário via NTP.
   69. Deve prover pelo menos dois tipos de backup: o primeiro simples gerando uma configuração a nível de linha de comando e um segundo que complementa o primeiro com o backup de arquivos importados para completar a configuração do sistema (páginas de erro, scripts e arquivos de blocos de endereço IP associados a provedores).
   70. Deve permitir o upgrade através de linha de comendo ou interface gráfica.
   71. Deve permitir o processo de upgrade em partições distintas.
   72. Deve suportar o update da base de dados de assinaturas de firewall de aplicação web, reputação IP e de endereços IP baseados em localização de forma separada e sem a necessidade de reinicialização do sistema.
   73. Deve suportar o update das bases de dados de assinaturas de forma programada indicando dia da semana e hora do dia.
   74. Deve suportar a configuração de um servidor de e-mail para o envio de e-mails de alerta.
   75. Deve implementar o agente de SNMP v1, V2c e 3 (RFC 3414).
   76. Deve permitir a configuração de eventos SNMP de, pelo menos, níveis de uso de CPU, memória e disco.
   77. Deve suportar o uso de certificados para suportar e gerenciar conexão de clientes usando os mesmos incluindo pelo menos: extensão TLS Server Name Indicator (SNI), armazenamento local de certificados (certificados X.509 v3 chaves privadas usadas pelos servidores), armazenamento e uso de certificados gerados de um dado CA, OCSP (Online Certificate Status Protocol), CRL (certificate revocation list) e solicitar certificado a um CA via SCEP (simple certificate enrollment protocol).
   78. O sistema deve possuir painel, via interface gráfica, que permita ao administrador visualização informações sobre o sistema incluindo pelo menos: estado do sistema (versão de firmware, utilização de CPU, utilização de memória, utilização de disco, número de conexões correntes, número de taxa de conexões, banda de entrada e de saída usada, logs mais recentes), balanceamento de carga (servidores reais, banda de entrada, de saída o número de conexões).
   79. Deve possuir, via interface gráfica, painel que mostre logs de eventos, de segurança e de tráfego de dados incluindo atividades dos administradores e de sistema.
   80. Deve implementar filtros que possibilitem a visualização de eventos de Configuração: indicando mudanças na configuração do sistema, usuário que fez a alteração, ação (edição, adição ou exclusão), configuração que foi alterada.
   81. Deve implementar filtros que possibilitem a visualização de eventos de Administração: indicando ações executadas por administradores.
   82. Deve implementar filtros que possibilitem a visualização de eventos de Sistema: indicando informações relevantes a operação, avisos e erros gerados pelo sistema.
   83. Deve implementar filtros que possibilitem a visualização de eventos de Usuário indicando atividades de autenticação de usuários, incluindo informações como: nome do usuário, grupo e política de autenticação usada.
   84. Deve implementar filtros que possibilitem a visualização de eventos de Verificação de saúde: indicando resultados de verificação de saúde, estado de validação de certificados, nome ou identificador do servidor real, estado da verificação: sucesso ou falha.
   85. Deve implementar filtros que possibilitem a visualização de eventos de Balanceamento de servidores: indicando que o número de conexões máximo foi atingido; identificador do servidor real, política relacionada ao evento.
   86. Deve implementar filtros que possibilitem a visualização de eventos de Balanceamento de Enlaces: indicando que limite de banda foi atingido; política relacionada ao evento.
   87. Deve implementar filtros que possibilitem a visualização de eventos de Balanceamento de Carga Global: identificador do servidor real, política relacionada ao evento.
   88. Deve implementar filtros que possibilitem a visualização de eventos de Firewall: política relacionada ao evento.
   89. Deve implementar filtros que possibilitem a visualização de eventos de Segurança - Reputação IP: indicando protocolo usado, endereços IP e portas de origem e destino, países de origem e destino do tráfego, nome da regra de segurança e ação tomada pela política.
   90. Deve implementar filtros que possibilitem a visualização de eventos de Segurança - DoS (Deny of Service): indicando protocolo usado, endereços IP e portas de origem e destino, países de origem e destino do tráfego, nome da regra de segurança e ação tomada pela política.
   91. Deve implementar filtros que possibilitem a visualização de eventos de Segurança - Firewall de aplicações web: indicando protocolo usado, endereços IP e portas de origem e destino, países de origem e destino do tráfego, nome da regra de segurança e ação tomada pela política e módulo de segurança de firewall para aplicações web relacionado (assinaturas, acesso a URL não permitidas, Cross Site script / Injeção SQL), URL e conteúdo do cabeçalho da mensagem HTTP.
   92. Deve implementar filtros que possibilitem a visualização de eventos de Segurança - Geo: indicando protocolo usado, endereços IP e portas de origem e destino, países de origem e destino do tráfego, nome da regra de segurança e ação tomada pela política.
   93. Deve implementar filtros que possibilitem a visualização de eventos de tráfego de balanceamento de carga de camada 4: protocolo, bytes in, bytes out, endereços IP e portas de origem e destino, países de origem e destino do tráfego.
   94. Deve implementar filtros que possibilitem a visualização de eventos de tráfego de balanceamento de carga de camada 7: protocolo, bytes in, bytes out, endereços IP e portas de origem e destino, países de origem e destino do tráfego, método HTTP, código de retorno HTTP, base URL, nome do cookie, nome do usuário, nome do grupo e estado de autenticação quando aplicável.
   95. Deve implementar filtros que possibilitem a visualização de eventos de tráfego de balanceamento global: protocolo, bytes in, bytes out, endereços IP e portas de origem e destino, países de origem e destino do tráfego, FQDN solicitado, endereço de resposta do DNS, nome da política usada.
   96. Para cada um dos eventos (logs de eventos, segurança e de tráfego) devem ser obrigatório indicação de: data, hora, nível de log, identificador da mensagem de log.
   97. Deve ser capaz de armazenar logs no próprio sistema.
   98. Deve permitir a seleção do menor nível de log a ser gravado localmente.
   99. Deve permitir a seleção do tipo de log a ser armazenado localmente (Eventos, Segurança e Tráfego) para evitar uso excessivo do disco.
   100. Deve ser capaz de enviar notificações de logs a servidor syslog.
   101. Deve permitir a seleção do menor nível de log a ser enviado para o servidor syslog.
   102. Deve permitir o envio de logs a servidor syslog no formato CSV.
   103. Deve permitir a seleção do tipo de log a ser enviado ao servidor syslog.
   104. A solução deve suportar o envio de alertas através de e-mails, estes alertas podem ser configurados de acordo com a categoria de eventos ou níveis de severidade.
   105. Deve suportar o envio de alertas através de e-mails relacionados a pelo menos eventos de: alta disponibilidade, administração, configuração, disco, verificação de saúde, expiração de certificados.
   106. Deve permitir e emissão de relatórios sob demanda ou programados.
   107. Deve suportar o envio via e-mail dos relatórios programados em formato PDF.
   108. Pelo menos os seguintes relatórios devem estar disponíveis no sistema:
        1. Para balanceamento de tráfego de servidores: políticas mais usadas e bytes associados, origens mais ativas e bytes associados e origens mais ativas por país e bytes associados, histórico de fluxo em bytes.
        2. Para balanceamento de tráfego entre enlaces: enlaces mais usados e bytes associados, histórico de fluxo em bytes; Reputação IP: destinos (alvos) mais frequentes com contagem associada, origens mais frequentes com contagem associada, origens mais frequentes com contagem e geografia associadas.
        3. DoS: destinos (alvos) mais frequentes com contagem associada.
        4. Geografias: destinos (alvos) mais frequentes com contagem associada, origens mais frequentes com contagem associada, origens mais frequentes com contagem associada e país.
        5. Firewall para aplicação web: destinos (alvos) mais frequentes com contagem associada, origens mais frequentes com contagem associada, origens mais frequentes com contagem e geografia associadas.
   109. Deve implementar características de redundância e alta disponibilidade em cluster do mesmo modelo, nos modos ativo-passivo e ativo-ativo.
   110. A formação do cluster deve permitir a sincronização de configuração e versão de sistema operacional entre os participantes.
   111. Possuir mecanismos de monitoramento de estado de interface que permita a alteração de estado do membro, de ativo para passivo, em caso de falha.
   112. Os participantes do cluster dever ser do mesmo modelo e ter a mesma versão de sistema operacional.
   113. Pelo menos as seguintes informações devem ser sincronizadas entre os membros do cluster: configuração principal (linha de comando), certificados X.509, arquivos de pedido de assinatura de certificados (certificate signing request files -CSR), chaves privadas, arquivos relativos a mensagens de erro, estados das conexões de nível 4, estados de persistência de nível 4 e nível 7.
   114. Quando em ativo-passivo apenas um dos membros encaminhará tráfego enquanto que o passivo só encaminhará tráfego caso haja falha no ativo.
   115. Quando em ativo-passivo o cluster ainda deverá manter a sincronização de sistema operacional e de configuração, minimizando impacto em caso de falha do ativo. Neste caso a transição deverá ser automática, sem intervenção externa ao cluster.
   116. Na configuração ativo-ativo todos os membros do cluster deverão encaminhar tráfego.
   117. Na configuração ativo-ativo o equipamento deverá ser capaz de compor um cluster com dois ou mais equipamentos da mesma família. Permitindo até 8 equipamentos.
   118. Deve permitir a configuração de parâmetro relativo à eleição do sistema primário (aquele em que as configurações são feitas e encaminhadas aos outros membros) dentro do mesmo cluster.
   119. Se necessário, deve permitir aplicar configurações em qualquer membro do cluster, independentemente se este é primário ou secundário.
   120. A sincronização da configuração do cluster pode ser realizada através de portas agregados.
   121. Deve possuir funcionalidades de virtualização, deve possibilitar a implementação de várias instâncias de sistema;
   122. Deve permitir o provisionamento de diferentes administradores para cada uma das instâncias de sistema.
   123. A solução deve permitir a encriptação/decriptação de sessões SSL no lugar dos servidores (processo conhecido como SSL Offload).
   124. Quando efetuando SSL Offload, deve agir como proxy dos servidores para fins de processamento SSL, usando certificados e chaves dos servidores para, pelo menos: autenticar os próprios servidores junto aos clientes, de-encriptar pedidos e encriptar respostas aos clientes.
   125. Deve possibilitar a implementação na rede como proxy SSL, neste caso desempenhando papel de proxy para os dois lados da conexão (clientes e servidores).
   126. Deve suportar pelo menos ciphers: RSA, PFS, ECDHE e eNull para SSL Offload.
   127. Deve suportar a configuração de ciphers para SSL Offload.
2. **Solução de Armazenamento de Logs e Relatórios**
   1. Deve possuir capacidade de receber ao menos 500 GigaBytes de logs diários.
   2. Não deve possuir limite de utilização de disco.
   3. Deve suportar acesso via SSH, WEB (HTTPS) e Telnet para o gerenciamento da solução.
   4. Deve possuir comunicação cifrada e autenticada com usuário e senha para solução de relatórios, tanto como para a interface gráfica de usuário e console de administração por linha de comandos (SSH).
   5. Permitir acesso simultâneo de administradores permitindo a criação de ao menos 2 (dois) perfis para administração e monitoração.
   6. Suportar SNMP versão 2 e versão 3 na solução de relatórios.
   7. Deve permitir a criação de administradores que acessem todas as instâncias de virtualização da solução de relatórios.
   8. Deve permitir habilitar e desabilitar, para cada interface de rede da solução de relatórios, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet.
   9. Deve possuir autenticação integrada a servidor Radius.
   10. Deve permitir a geração de relatórios em tempo real, para a visualização de tráfego observado, nos formatos: mapas geográficos e tabela.
   11. Deve possuir autenticação integrada ao Microsoft Active Directory.
   12. Deve possuir definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.
   13. Possuir mecanismo para que logs antigos sejam removidos automaticamente.
   14. Permitir a importação e exportação de relatórios.
   15. Deve possuir a capacidade de criar relatórios nos formatos PDF.
   16. Deve ser possível exportar os logs em CSV.
   17. Deve gerar logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.
   18. Os logs gerados pelos appliances devem ser centralizados nos servidores de gerência, mas a solução deve oferecer também a possibilidade de utilização de um syslog externo ou similar.
   19. A solução deve possuir relatórios pré-definidos.
   20. Possuir envio automático de logs para um servidor FTP externo a solução.
   21. Permitir de forma centralizada visualizar os logs recebidos por um ou vários dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste log.
   22. Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados.
   23. Deve possuir a capacidade de personalização de gráficos como barra, linha e tabela para inserção aos relatórios.
   24. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em realtime.
   25. Dever ser possível fazer download dos arquivos de logs recebidos.
   26. Deve possuir agendamento para gerar e enviar automaticamente relatórios.
   27. Deve permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades.
   28. Permitir o envio de maneira automática de relatórios por e-mail.
   29. Permitir programar a geração de relatórios, conforme calendário definido pelo administrador.
   30. Deve ser possível definir filtros nos relatórios.
   31. Deve ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros.
   32. Deve gerar alertas automáticos via Email, SNMP e Syslog baseados em eventos como ocorrência como log, severidade de log, entre outros.
   33. Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios.
   34. Deve ter a capacidade de visualizar na GUI da solução de relatórios informações do sistema como licenças, memória, disco, uso de CPU, taxa de logs por segundo recebidos, total de logs diários recebidos, alertas gerados entre outros.
   35. Deve permitir ver em tempo real os logs recebidos
   36. Deve permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino.
   37. Deve possuir relatório detalhado de prevenção de perda de dados (DLP).
   38. Deve possuir relatório de VPN.
   39. Deve possuir relatório de Sistemas de prevenção de intrusão (IPS).
   40. Deve possuir relatório de reputação do cliente.
   41. Deve possuir relatório de análise de segurança do usuário.
   42. Deve possuir relatório de avaliação da ameaça cibernética.
3. **Data Center - padrão TIER III**

O datacenter onde os componentes servidores da *PLATAFORMA* serão instalados deverá estar localizado no território nacional e ter uptime superior a 99,749%, redundância parcial de refrigeração e fornecimento de energia e ocorrências de indisponibilidade inferiores a 20 por ano, sendo aceita a comprovação por meio de certificação TIER 3.

O datacenter deve atender no mínimo as seguintes características:

* 1. Deve ser atendido por no mínimo duas empresas de telecomunicações.
  2. Os cabos das empresas de telecomunicação devem vir por rotas distintas até o Data Center.
  3. Deve estar em zonas de proteção contra incêndios.
  4. Possuir sistemas de energia e ar-condicionado distintos.
  5. As conexões entre as salas devem ser feitas via fibra ou pares metálicos redundantes.
  6. Prover pelo menos a redundância elétrica N+1.
  7. Deve possuir disponibilidade mínima de 99,749% e até 72 horas de proteção contra interrupção de energia.

**ITEM 03) ESPECIFICAÇÃO TÉCNICA DO MODEM WI-FI PORTÁTIL**

O MODEM WI-FI PORTÁTIL deve apresentar no mínimo as seguintes características:

1. Especificações básicas

1.1. Possuir suporte à tecnologia e-sim;

1.2. Apresentar compatibilidade com os seguintes requisitos:

1.2.1. Para conectividade o Dispositivo deve suportar:

1.2.1.1. Ao menos uma das tecnologias de rede de acesso definidas pelo 3GPP na seguinte lista não exaustiva:

1.2.1.2. GERAN,

1.2.1.3. UTRAN,

1.2.1.4. E-UTRAN.

1.2.1.5. UDP over IP (sujeito ao suporte correto de tecnologia de rede de acesso)

1.2.1.6. TCP over IP (sujeito ao suporte correto de tecnologia de rede de acesso)

1.2.2. Para controle de conexão de rede, o Dispositivo deve suportar:

1.2.2.1. Detalhes RPLMN (LAC/TAC, NMR).

1.2.2.2. QoS (falhas, duração, energia, localização).

1.2.2.3. Gerenciamento SMS.

1.2.2.4. Nova seleção de rede após atualização do SIM/USIM.

1.2.3. Para reportar a um servidor o Dispositivo deve suportar:

1.2.3.1. SMS-PP MO como definido em e SMS-PP MO como definido ou

1.2.3.2. BIP como definido em DEV4

1.2.4. O Dispositivo deve suportar:

1.2.4.1. USSD

1.2.5. Para Gerenciamento de Perfil e Plataforma o Dispositivo deve suportar:

1.2.5.1. SMS-PP MT como definido em, e SMS-PP MT como definido em ou

1.2.6. BIP (sujeito ao suporte correto de tecnologia de rede de acesso) como definido em incluindo suporte aos comandos:

1.2.6.1. OPEN CHANNEL (UDP e TCP over IP)

1.2.6.2. CLOSE CHANNEL

1.2.6.3. RECEIVE DATA

1.2.6.4. SEND DATA

1.2.6.5. GET CHANNEL STATUS

1.2.6.6. ENVELOPE (EVENT DOWNLOAD – Dados disponíveis)

1.2.6.7. ENVELOPE (EVENT DOWNLOAD – Status do canal)

1.2.7. O Dispositivo deve conter um valor de IMEI (International Mobile Equipment Identity) único compatível com o formato definido na ETSI TS 123 003.

1.2.8. O valor do IMEI deve ser copiado diretamente do TERMINAL RESPONSE do comando Provide Local Information (ver ETSI TS 102 223 e ETSI TS 124 008).

1.2.9. O dispositivo deve suportar, no mínimo, o seguinte conjunto de comandos (além dos comandos BIP), conforme definido em ETSI TS 102 223 e 3GPP TS 31.111.

1.2.10. Comandos SAT básicos (TERMINAL PROFILE, FETCH, TERMINAL RESPONSE).

1.2.11. PROVIDE LOCAL INFORMATION (informações de localização, IMEI, NMR, data e hora, tecnologia de acesso, pelo menos).

1.2.12. SEND SHORT MESSAGE:

1.2.13. POLL INTERVAL, POLLING OFF, TIMER MANAGEMENT [pelo menos um cronômetro], ENVELOPE (EXPIRAÇÃO DO TEMPORIZADOR).

1.2.14. SET UP EVENT LIST e ENVELOPE (EVENT DOWNLOAD status de localização, chamada conectada, chamada desconectada, tecnologia de acesso alterada, rejeição de rede).

1.2.15. ENVELOPE (SMS-PP DOWNLOAD).

1.2.16. REFRESH Command (ao menos modo 4 – “UICC reset”).

1.2.17. O dispositivo deve estar em conformidade com o document GSMA – EICTA “Security Principles Related to Handset Theft”.

1.2.18. O dispositivo pode recuperar o EID definido na seção 2.2.2 desta especificação do eUICC e deve suportar os seguintes comandos, conforme descrito em:

1.2.18.1. AT+CCHO (Canal lógico aberto)

1.2.18.2. AT+CCHC (Fechar Canal Lógico)

1.2.18.3. AT+CGLA (Acesso de canal lógico UICC genérico)

1.2.19. O dispositivo deve suportar os seguintes comandos para todos os fins genéricos:

1.2.19.1. AT+CRSM (Acesso restrito ao SIM)

1.3. Permitir remotamente a troca de operadora;

1.4. Possuir chipset Qualcomm MDM 9307;

1.5. Possuir no mínimo 2 (dois) Slots:

• Um, para SIM 3FF (micro-SIM card);

• E outro, para Micro SD (de até 32 GB).

1.6. Ter memória mínima de 2 Gb;

1.7. Possibilitar no mínimo 10 (dez) dispositivos conectados simultaneamente.

2. Especificações de rádio frequência (RF)

2.1. Possuir no mínimo padrão de redes de comunicação móveis LTE (Long Term Evolution):

• FDD Banda 3/7;

• TDD Banda 38/39/41.

2.2. Fornecer no mínimo as seguintes larguras de banda do canal: 1.4/3/5/10/15/20 MHz

2.3. Fornecer Wi-Fi padrão 802.11b/g/n de 2,4 GHz

2.4. Possuir sistema MIMO: DL 2x2

2.5. Taxa de transferência:

• Possuir LTE categoria 4: 150 Mbps / 50 Mbps;

• Apresentar taxa de transferência de Wi-Fi de 150 Mbps.

2.6. Possuir antena LTE modo 1T2R, e Wi-Fi modo 1T1R

3. Deve suportar no mínimo os sistemas operacionais abaixo:

3.1. Linux;

3.2. Mac OS;

3.3. Windows XP/ Windows Vista/ Windows 7/ Windows 8.

4. Compatibilidade / Manutenção

4.1. Permitir configuração de data e hora;

4.2. Permitir opção de reset;

4.3. Permitir restauração das configurações de fábrica;

4.4. Possuir diagnóstico em rede: Ping e trace route.

5. Possuir certificação ISO 9001.

6. Equipamento deve ser homologado na Anatel.

7. Possuir as seguintes funções:

7.1. SMS (Short Message Service - serviço de mensagens curtas);

7.2. Estatísticas de fluxo;

7.3. WPS (Wireless Priority Service – serviço de prioridade sem fio);

7.4. WDS (Wireless Distribution System - Sistema de distribuição sem fio);

7.5. DHCP (Dynamic Host Configuration Protocol - protocolo de configuração dinâmica de hosts);

7.6. DNS (Domain Name System - sistema de nomes de domínio);

7.7. DDNS (DNS dinâmico);

7.8. Encaminhamento de portas;

7.9. uPnP (Plug and Play universal);

7.10. Firewall (política de segurança em rede);

7.11. Wi-Fi storage: Armazenamento de dados da rede Wi-Fi no cartão de memória;

7.12. OTA (Over-the-Air): Utilizado para determinar o desempenho do sistema sem fio nos dispositivos habilitados;

7.13. APK (Android Package): É um arquivo de pacote destinado ao sistema operacional Android.

8. Características físicas e gerais

8.1. Deve acompanhar um cabo USB para que possa carregar a bateria quando conectado à uma porta USB energizada, com 5 V e até 1 A de saída;

8.2. Bateria 3000 mAh;

8.3. Tempo máximo de trabalho: 13 horas;

8.4. Tempo máximo em standby: 500 horas;

8.5. Botão liga/desliga;

8.6. Botão WPS (Wireless Priority Service);

8.7. Uma porta USB 2.0 micro-B;

8.8. Temperatura de operação: -10 ºC ~ 60 ºC;

8.9. Dimensões: 85x68x16 mm;

8.10. Peso aproximado: 150 gramas (com bateria).

8.11. Especificação do e-sim fornecido juntamente com o Dispositivo de Acesso

8.11.1. Deverá ser fornecido no formato triplo corte (2FF, 3FF e 4FF).

8.11.2. Deverá ser compatível com o padrão eUICC estabelecido pela GSMA.

8.11.3. Deverá possuir capacidade mínima de 512Kb.

8.11.4. Arquitetura composta pelos seguintes itens:

8.11.5. eUICC

8.11.6. RAM/RFM/Keys;

8.11.7. SM/Data/Keys;

8.11.8. SMC

8.11.9. MNO1

8.11.10. Applets;

8.11.11. RAM/RFM/Keys;

8.11.12. File System;

8.11.13. NAA Data;

8.11.14. Policies.

8.11.15. MNO 2

8.11.16. Applets;

8.11.17. RAM/RFM/Keys;

8.11.18. File System;

8.11.19. NAA Data;

8.11.20. Policies.