TERMO DE REFERÊNCIA

1. OBJETO

Registro de Preços para eventual e futura contratação de solução de tecnologia que viabilize a conectividade gerenciada e controlada para que alunos e professores possam acessar as plataformas educacionais digitais definidas pela gestão da Rede Municipal de Ensino do Município de Goiana-PE.

2. DA JUSTIFICATIVA PARA CONTRATAÇÃO DO OBJETO

A COVID-19 passou a exigir dos setores público e privado a necessidade de implementação de infraestrutura e ferramentas para viabilização de um modelo de educação remota. Para suprir essa demanda, além do esforço e comprometimento de alunos, professores e servidores, em contrapartida a Secretaria de Educação e Inovação do município vem implementando diversas medidas para enfrentar essa nova realidade e, nesse contexto vem realizando esforços para disponibilizar uma infraestrutura que comporte a transmissão, acompanhamento e gestão do conteúdo transmitido.

Para permitir o acesso à educação em casa é necessário disponibilizar a alunos e professores o acesso (internet) a conteúdos públicos ou a servidores de conteúdo digital utilizados pela Secretaria de Educação e Inovação ou ainda a ambientes disponibilizados por instituições terceiras, como o Ministério da Educação, fundações ou a ambiente digital de empresas fornecedoras.

Por fim, cabe à Secretaria de Educação Inovação do município a gestão dos acessos aos conteúdos e a gestão do uso e consumo da internet disponibilizada, como forma de assegurar que o recurso cedido seja utilizado exclusivamente para fins educacionais. Desta forma, haverá a garantia da correta aplicação dos recursos destinados nesta ação.

Um grande passo para se obter sucesso em medidas de gestão, especialmente em se tratando da rede pública de ensino, ampla e complexa, é estar amparado por ferramentas de suporte e de informação, ou seja, os gestores deverão contar com uma plataforma tecnológica onde possam ter informações sobre a aplicação e utilização dos acessos à internet.

A necessidade de visualização de dados e de medição de desempenho na utilização da infraestrutura disponibilizada aos alunos e professores é parte da gestão escolar. Os sistemas de informação subsidiam gestores em suas decisões e escolhas, permitindo uma melhor tomada de decisão e auxílio em políticas educacionais. A exigência cada vez maior em aperfeiçoar os níveis dos resultados educacionais, bem como gerar e fortalecer mecanismos de transparência e responsabilização para os cidadãos e partes interessadas geram a necessidade da administração pública em implantar plataformas informacionais que permitam desenvolver e implementar indicadores de desempenho.

Para isso é necessário a implantação de plataforma composta de hardware, software e serviço técnico especializado para monitoramento e gestão da conectividade de alunos e professores. O serviço prestado permitirá à Secretaria de Educação e Inovação a gestão da utilização de recursos pelos alunos, professores e colaboradores da Secretaria de Educação envolvidos no processo.

Afora isso, a **RESOLUÇÃO CONSELHO NACIONAL DE EDUCAÇÃO CNE/CP Nº 2, DE 10 DE DEZEMBRO DE 2020** em sua Ementa assim:

> *Institui Diretrizes Nacionais orientadoras para a implementação dos dispositivos da Lei nº 14.040, de 18 de agosto de 2020, que estabelece normas educacionais excepcionais a serem adotadas pelos sistemas de ensino, instituições e redes escolares, públicas, privadas, comunitárias e confessionais, durante o estado de calamidade reconhecido pelo Decreto Legislativo nº 6, de 20 de março de 2020.*

Na **Seção IV - Do Retorno às Atividades Presenciais assim está exposto:**

Art. 9º A volta às aulas presenciais deve ser gradual, por grupos de estudantes, etapas ou níveis educacionais, em conformidade com protocolos produzidos pelas autoridades sanitárias locais, pelos sistemas de ensino, secretarias de educação e instituições escolares, com participação das comunidades escolares, considerando as características de cada unidade educacional, observando regras de gestão, de higiene e de distanciamento físico de estudantes, de funcionários e profissionais da educação, com

escalonamento de horários de entrada e saída para evitar aglomerações, e outras medidas de segurança recomendadas.

§ 1º Tomadas as medidas de segurança determinadas e regulamentadas pelas autoridades locais, os sistemas de ensino, as secretarias de educação e as instituições escolares, conforme as circunstâncias, definem o calendário de retorno gradual para as diferentes etapas da Educação Básica.

§ 2º Devem ser especialmente planejadas as atividades dos professores, presencial e não presencial, em função do retorno parcial escalonado dos estudantes ao ambiente escolar.

Art. 10. As Secretarias Estaduais e Municipais de Educação têm competência e responsabilidade para definir medidas de retorno às aulas, bem como para oferecer atividades não presenciais e/ou de ensino flexível híbrido no retorno gradual às aulas presenciais, respeitando os protocolos sanitários locais, considerando os diferentes impactos e tendências da pandemia.

§ 1º Fica facultado aos sistemas de ensino, em caráter excepcional e mediante disponibilidade de vagas na rede escolar pública, possibilitar ao concluinte do Ensino Médio matricular-se para períodos de estudos flexíveis, presenciais ou híbridos, de até 1 (um) ano letivo suplementar, no ano subsequente ao afetado pelo estado de calamidade pública.

§ 2º Atividades presenciais devem ser retomadas com o seguimento das medidas de proteção à comunidade escolar, sobretudo aos estudantes, funcionários, professores e demais profissionais da educação, e suas famílias, a partir de uma avaliação dos benefícios e riscos associados a questões sociais e econômicas, considerando critérios sanitários específicos, conforme as peculiaridades locais de cada instituição escolar.

Art. 11. Cabe às secretarias de educação e a todas as instituições escolares:

I – planejar a reorganização dos ambientes de aprendizagem, comportando tecnologias

disponíveis para o atendimento do disposto nos currículos;

4II – realizar atividades on-line síncronas e assíncronas de acordo com a disponibilidade tecnológica;

III – realizar atividades de avaliação on-line ou por meio de material impresso entregue desde o período de suspensão das aulas; e

*IV – **utilizar mídias sociais de longo alcance (WhatsApp, Facebook, Instagram etc.) para estimular e orientar os estudos, pesquisas e projetos que podem ser computados no calendário e integrar o replanejamento curricular**.*

§ 1º As atividades referidas no caput devem, conforme as peculiaridades e exigências locais, garantir e condizer com o calendário escolar dos anos letivos 2020 e 2021 devidamente reorganizado, por conta da afetação pelo estado de calamidade pública, obedecendo os princípios dispostos no art. 206 da Constituição Federal.

§ 2º O disposto neste artigo deve, notadamente, assegurar a igualdade de condições para o acesso e a permanência escolar, contando com a participação das comunidades escolares para sua definição.

§ 3º Cabe às instituições e redes escolares públicas, privadas, comunitárias e confessionais promover, no âmbito de sua atuação, estruturas suficientes para efetivar as garantias e exigências estabelecidas no caput deste artigo.

Art. 12. Os sistemas de ensino devem criar protocolos pedagógicos, quando possível, em conformidade com decisões tomadas por comitês estaduais articulados com seus respectivos municípios e por comitês promovidos por comissões escolares municipais, objetivando o retorno gradual em respeito a regras sanitárias de prevenção.

§ 1º Os sistemas de ensino, as secretarias de educação e as instituições escolares devem planejar o retorno a atividades presenciais, segundo número limitado de alunos em cada sala de aula, conforme protocolos locais e condições de funcionamento efetivo de cada unidade escolar, garantida a reorganização dos horários e dias de atendimento aos estudantes e às famílias.

§ 2º Cabe aos pais ou responsáveis legais, em comum acordo com a escola e com as regras estabelecidas pelos sistemas de ensino, a opção pela permanência do estudante em atividade não presencial, mediante compromisso das famílias ou responsáveis pelo cumprimento das atividades e avaliações previstas no replanejamento curricular.

Art. 13. No retorno às atividades presenciais, os sistemas de ensino, as secretarias de educação e as instituições escolares devem assegurar, em conformidade com as necessidades específicas, o acolhimento aos estudantes e a preparação socioemocional de todos os professores, demais profissionais da educação e funcionários, que podem enfrentar situações excepcionais na atenção aos estudantes e respectivas famílias.

§ 1º No processo de retorno gradual às atividades presenciais, as instituições escolares devem realizar o acolhimento e a reintegração social dos professores, estudantes e suas famílias, e manter um amplo programa para formação continuada dos professores, visando a prepará-los para este trabalho de integração.

§ 2º As atividades de acolhimento devem, na medida do possível, envolver a promoção de diálogos com trocas de experiências sobre o período vivido (considerando as diferentes percepções das diferentes faixas etárias), bem como a organização de apoio pedagógico, de diferentes atividades físicas e de ações de educação alimentar e nutricional, entre outras.

3. OBJETIVOS

A contratação da solução definida neste Termo de Referência tem como foco alcançar os seguintes objetivos:

- Garantir que os recursos financeiros da Educação sejam aplicados exclusivamente para fins educacionais;
- Prover a conectividade aos alunos da rede municipal de educação garantindo acesso aos recursos de educação remota fornecidos pela secretaria de educação;
- Garantir a correta utilização dos recursos de acesso à internet por parte dos alunos e professores;
- Garantir que apenas conteúdos autorizados pela Secretaria de Educação possam ser acessados pelos alunos;
- Monitorar o tipo e o volume de tráfego realizado dentro da infraestrutura de educação disponibilizada, permitindo ajustes e melhorias constantes;
- Permitir a gestão e monitoramento dos equipamentos e dos recursos oferecidos aos alunos da educação remota;
- Minimizar o problema da falta de cobertura e ausência de conectividade em localidades específicas, contando com redes alternativas que se somam para melhor atendimento dos usuários nas localidades com mais restrições de acesso;
- Disponibilizar um mecanismo de acesso que viabilize acesso a conteúdos digitais por diversos canais, tais como: navegadores web, aplicativo mobile, dentre outros;

4. TOPOLOGIA DA SOLUÇÃO

A CONTRATADA será responsável por toda a infraestrutura de conectividade desde o fornecimento dos Dispositivos de Acesso, os meios de acesso ao conteúdo, filtros de acesso e infraestrutura de segurança.

Todo o tráfego de dados demandados pelos usuários deverá ser direcionado para a Solução de Gestão e Controle dos Acessos e Conectividade da CONTRATADA. Esta realizará os filtros ou restrições de acesso aplicáveis a cada perfil de usuário, (aluno por série, professor ou servidor), de acordo com as autorizações definidas no momento do cadastro de cada usuário da Secretaria.

O Dispositivo de Acesso irá disponibilizar um sinal Wi-Fi, permitindo assim, que o aluno ou professor tenha acesso à internet em qualquer lugar, desde que esteja sob área de cobertura de uma das redes de conectividade utilizadas pela CONTRATADA. Por meio do Dispositivo de Acesso o aluno terá acesso restrito e controlado à internet seguindo as regras de acesso definidas pela CONTRATANTE.

A Solução de Gestão de Controle dos Acessos e Conectividade fornecida pela CONTRATADA realizará toda a checagem de autorização permitindo o acesso dos alunos apenas aos conteúdos online autorizados ou aos servidores de conteúdo da Secretaria de Educação. Toda política de acesso será definida pela CONTRATANTE e implementada pela CONTRATADA.

A solução de gestão e controle dos acessos e conectividade deve estar munida de equipamentos e softwares capazes de processar todo o tráfego, 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.

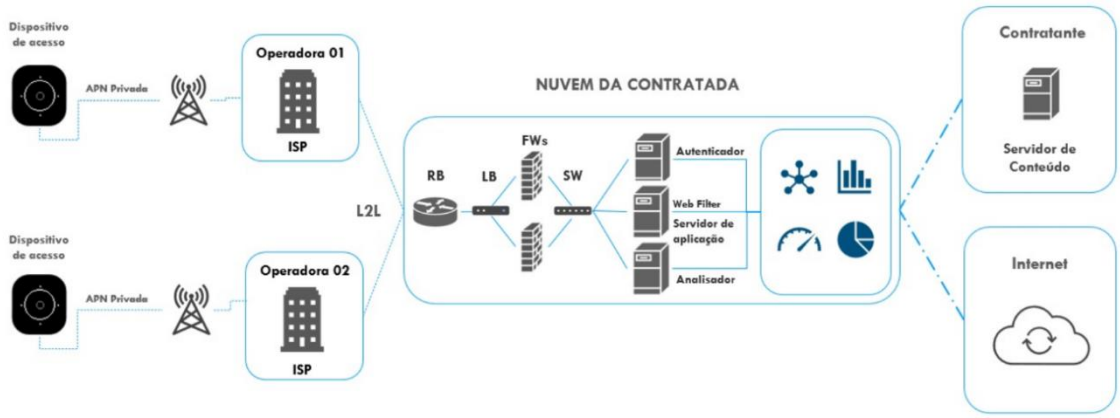

Figura 1: Topologia da solução.

5. DESCRIÇÃO DOS SERVIÇOS E DA SOLUÇÃO TECNOLÓGICA

5.1 A solução é composta por dispositivo de hardware, software e serviços técnicos especializados com o objetivo de permitir o acesso aos recursos de educação remota, fornecidos pela Secretaria de Educação e Inovação do município para 10.000 alunos e 1.000 professores.

5.2 A licitação contratará os seguintes itens em lote único, os itens serão descritos abaixo:

ITEM	DESCRIÇÃO	UNIDADE	QUANT.
1	SERVIÇO DE CAPACITAÇÃO DE PROFESSORES EM "AULA INTERATIVA"	SERVIÇO	1.000
2	IMPLANTAÇÃO E ATIVAÇÃO DA SOLUÇÃO DE GESTÃO E CONTROLE DOS ACESSOS E CONECTIVIDADE	SERVIÇO	1
3	DISPOSITIVO DE ACESSO	LOCAÇÃO MENSAL	1.000
4	SERVIÇO GERENCIADO DE ACESSO REMOTO A CONTEÚDO EDUCACIONAL	SERVIÇO MENSAL	11.000

5.3 Não faz parte da solução oferecida pela CONTRATADA aquisição de dispositivos/equipamentos como notebooks, tablets ou smartphones, que poderão ser objeto de processo licitatório distinto.

5.4 **Serviço de Capacitação de Professores em Aula Interativa**

5.4.1 CONTRATADA deverá capacitar os professores na evolução da Educação, treinando-os nas novas tecnologias de ensino, o curso deve conter no mínimo os temas abaixo:

5.4.1.1 Educação EAD e a necessidade de adaptação dos educadores;

5.4.1.2 Tendências e desafios no novo cenário da educação digital;

5.4.1.3 Marketing digital e redes sociais;

5.4.1.4 Como produzir conteúdo de forma assertiva para a educação;

5.4.1.5 Utilização da comunicação e eficiência na gravação de aulas;

5.4.1.6 Novos equipamentos, ferramentas e sistemas tecnológicos para produção de conteúdo;

5.4.1.7 Como utilizar a Solução de Gestão e Controle dos Acessos e Conectividade;

5.4.2 A CONTRATADA deve realizar capacitação de até 08 horas com aulas remotas, realizadas em plataforma tecnológica de EAD própria.

5.4.3 As aulas devem ser realizadas em horário a ser definido entre CONTRATANDA e CONTRATANTE sempre em horário comercial.

5.4.4 As aulas devem ser gravadas para posterior visualização de todos os colaboradores da CONTRATANTE.

5.4.5 Além das videoaulas a CONTRATADA deverá disponibilizar material de apoio a plataforma customizada para o curso.

5.5 Solução de Gestão e Controle dos Acessos e Conectividade:

5.5.1 A Solução de Gestão e Controle dos Acessos e Conectividade é uma plataforma 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.

5.5.2 A Solução de Gestão e Controle dos Acessos e Conectividades deve permitir a criação de perfis de acordo com a necessidade da CONTRATANTE, onde estarão todas as parametrizações e customizações necessárias para acesso ao conteúdo por parte dos alunos, professores e colaboradores da Secretaria de Educação.

5.5.3 Os Perfis deverão possuir lista de liberação de acesso (whitelist) específicos. Cada série da educação básica deverá possuir um respectivo Perfil válido para todos os alunos desta série.

5.5.4 Os Professores deverão possuir Perfil específico, com acesso gerenciado e controlado a partir de uma lista de endereços bloqueados (blacklist).

5.5.5 A Solução de Gestão e Controle de Acesso e Conectividade 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:

5.5.5.1 Das escolas: Nome da escola, Endereço completo da escola, Gestor da escola, E-mail do gestor da escola e Diretor da escola;

5.5.5.2 Das turmas: Nome da escola, Série e Número da turma;

5.5.5.3 Dos alunos: Nome da escola, Série, Ano letivo, Número da turma, Nome do aluno, Matrícula, Ano de nascimento e Endereço.

5.5.6 A Solução de Gestão e Controle de Acesso e Conectividade fornecida pela CONTRATADA deve possuir sistema de varredura e auditoria de inconsistências nos dados fornecidos pela CONTRATANTE, apresentando:

5.5.6.1 Relatório de cadastros duplicados ou aluno com mais de um cadastro.

5.5.6.2 Relatório de cadastros incompletos.

5.5.6.3 Relatório de duplicidade em turmas e escolas.

5.5.6.4 Para o caso de duplicidade ou inconsistência nos cadastros o sistema deve apresentar alarme informando o erro, para que medidas cabíveis possam ser tomadas

5.5.7 A CONTRATADA deve possuir equipe técnica especializada na parametrização da plataforma que será responsável por incluir o Banco de Dados disponibilizado pela CONTRATANTE.

5.5.8 Os requisitos mínimos da Solução de Gestão e Controle dos Acessos e Conectividade estão especificados no ANEXO 1 e as funcionalidades serão detalhadas neste item.

5.5.9 A Solução de Gestão e Controle de Acesso e Conectividade 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.

5.5.10 Características Gerais da Solução de Gestão e Controle de Acesso e Conectividade:

5.5.10.1 Deve possuir mecanismos de gerenciamento de senhas, expiração, bloqueio, alteração, reset, histórico dos colaboradores, alunos e professores da secretaria de educação.

5.5.10.2 Deve permitir mecanismos de extração, transformação e carga de dados.

5.5.10.3 Todas as aplicações e infraestrutura tecnológica necessária para o pleno funcionamento da Solução de Gestão e Controle de Acesso devem estar instaladas em Data Center TIER III fornecido pela CONTRATADA conforme especificado no ANEXO I.

5.5.10.4 A Solução de Gestão e Controle dos Acessos e Conectividade deve possuir 4 tipos de Perfis de Utilização: Administrador, Professor, Aluno e Cadastrador Detalhados a seguir:

5.5.10.4.1 O Perfil de Utilização Administrador será utilizado pela CONTRATADA para realizar criação e parametrização dos usuários na Plataforma de Gerenciamento de acordo com os Perfis de Utilização definidos.

5.5.10.4.2 O Perfil de Utilização Professor será utilizado pela CONTRATANTE e deve permitir a visualização dos endereços de acesso ao conteúdo e materiais definidos pela Secretaria de Educação e visualização dos conteúdos de todas as turmas de responsabilidade do professor.

5.5.10.4.3 O Perfil de Utilização Aluno deve permitir a visualização do conteúdo definido para sua respectiva turma e matéria.

5.5.10.4.4 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.

5.5.10.5 A Solução de Gestão e Controle dos Acessos e Conectividade 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 serão executadas pelo Service Desk da CONTRATADA.

5.5.10.6 A Solução de Gestão e Controle dos Acessos e Conectividade é responsável por garantir a conectividade ao conteúdo acessado pelos alunos seja o definido pelas regras de segurança da Secretaria de Educação.

5.5.10.7 A Solução de Gestão e Controle dos Acessos e Conectividade deve monitorar os Dispositivos de Acesso.

5.5.10.8 A Solução de Gestão e Controle dos Acessos e Conectividade 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 CONTRATANDA por meio de Ordem de Serviço aberta pela CONTRATANTE.

5.5.10.9 A Solução de Gestão e Controle dos Acessos e Conectividade 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.

5.5.10.10 A Solução de Gestão e Controle dos Acessos e Conectividade deve permitir inserir os dias da semana e horários em que o conteúdo estará liberado para acesso dos alunos.

5.5.10.11 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.

5.5.10.12 Deve conter filtros na tela de acesso com o intuito de facilitar a pesquisa e visualização dos conteúdos.

5.5.10.13 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.

5.5.10.14 Todos os dados de status, localização e nível de utilização do Dispositivo de Acesso e do volume de consumo de internet devem ser consolidadas em relatórios diários, semanais e mensais.

5.5.10.15 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.

5.5.10.16 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.

5.5.10.17 Deve gerar alarmes de usuários com utilização fora do compliance permitindo ações da CONTRATANTE seja com alunos, professores ou servidores da Secretaria de Educação.

5.5.10.18 Deve possibilitar a restrição de forma automática do uso do Dispositivo de Acesso sempre que ferir regras do compliance ou a pedido da CONTRATANTE.

5.5.10.19 A Plataforma deve possuir menu no dashboard com no mínimo as seguintes opções, relacionadas ao gerenciamento dos Dispositivos de Acesso:

5.5.10.19.1 Bloquear Dispositivo de Acesso.

5.5.10.19.2 Reativar Dispositivo de Acesso.

5.5.10.19.3 Suspender Dispositivo de Acesso.

5.5.10.19.4 Cancelar Dispositivo de Acesso.

5.5.10.19.5 Troca de ICCID.

5.5.10.19.6 Desbloquear Dispositivo de Acesso.

5.5.10.19.7 Substituir Dispositivo de Acesso.

5.5.10.19.8 Migrar proprietário do Dispositivo de Acesso.

5.5.10.19.9 Informações do cliente.

5.5.10.19.10 Manutenção de quarentena.

5.5.11 Do aplicativo ou ambiente web fornecido pela CONTRATADA

5.5.11.1 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:

5.5.11.1.1 No caso de APP ser compatível com os sistemas operacionais Android e iOS.

5.5.11.1.2 No caso de Web ser compatível com os principais navegadores de mercado.

5.5.11.1.3 Permitir a identificação e preenchimento automáticos dos dados dos Dispositivos de Acesso através da leitura dos seus códigos de barras ou QR Code.

5.5.11.1.4 Possuir campos digitáveis para inserção dos códigos de forma manual, quando necessário.

5.5.11.1.5 Deve exigir credenciais de acesso aos cadastradores e liberar a vinculação apenas dos alunos cujas turmas foram definidas para o mesmo.

5.5.11.1.6 Trazer as opções de escola, séries, turmas e nome do aluno.

5.5.12 Implantação e Ativação da Solução de Gestão e Controle dos Acessos e Conectividade:

5.5.12.1 A implantação e ativação da solução de Gestão e Controle dos Acessos e Conectividade é um serviço realizado pela CONTRATADA no início do projeto composto por parametrização da Solução de Gestão e Controle de Acesso e preparação do ambiente de TI (CLOUD). Trata-se de um serviço realizado unicamente, no início da contratação.

5.5.12.2 A implantação e ativação da Solução de Gestão e Controle dos Acessos e Conectividade é responsável por viabilizar tecnicamente o cadastramento de todos os alunos, professores e dos componentes que permitem a conexão ao ambiente tecnológico de educação remota.

5.5.12.3 Para o serviço de implantação e ativação da Solução de Gestão e Controle dos Acessos e Conectividade a CONTRATADA deverá:

5.5.12.3.1 Levantar e parametrizar os requisitos de segurança e acesso dos alunos, professores e demais colaboradores da CONTRATANTE;

5.5.12.3.2 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.

5.5.12.3.3 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.

5.6 Dispositivo de Acesso:

5.6.1 O Dispositivo de Acesso é o equipamento por meio do qual o aluno terá acesso ao conteúdo educacional. Estes serão disponibilizados pela CONTRATADA em modelo de locação aos alunos e professores da rede municipal.

5.6.2 O Dispositivo de Acesso fornecido pela CONTRATADA deve realizar a conexão à internet por meio das redes móveis (3G ou 4G) de todas operadoras disponíveis nas localidades, priorizando sempre a operadora com melhor conectividade.

5.6.3 O Dispositivo de Acesso fornecido deve conectar o tablet, notebook ou smartphone do aluno à internet por meio de uma rede wi-fi criada pelo equipamento. O acesso do aluno à rede educacional deve ser direto e restrito ao perfil definido pela Secretaria de Educação e Inovação do Município.

5.6.4 O Dispositivo de Acesso deverá ser ativado por equipe da CONTRATANTE, após treinamento ministrado pela equipe da CONTRATADA.

5.6.5 Da Ativação do Dispositivo de Acesso:

5.6.5.1 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 Solução de Gestão e Controle dos Acessos e Conectividade.

5.6.5.2 Os Dispositivos de Acesso devem ser entregues com todos os recursos necessários para a conectividade. Bastando aos colaboradores da CONTRATANTE atribuir a cada aluno o Dispositivo de Acesso correspondente à turma e o perfil.

5.6.6 O Dispositivo de Acesso deve possuir no mínimo as características descritas no ANEXO I.

5.6.7 O Dispositivo de Acesso deve ser disponibilizado lacrado com todos os componentes necessários e configurado para permitir conectividade limitada aos alunos, permitindo acesso apenas a conteúdos contidos na política de segurança da Secretaria de Educação.

5.6.8 O Dispositivo de Acesso será distribuído aos alunos e professores durante o processo de ativação do dispositivo pela equipe da CONTRATANTE.

5.7 SERVIÇO GERENCIADO DE ACESSO REMOTO A CONTEÚDO EDUCACIONAL O Serviço Gerenciado de Acesso Remoto a Conteúdo Educacional deverá manter a conectividade de alunos e professores dentro de níveis de serviços estabelecidos neste documento e será prestado pelo período de 12 meses.

5.8 É um serviço mensal composto por mão de obra técnica especializada para o suporte e manutenção da Solução de Gestão e Controle dos Acessos de Conectividade fornecida pela CONTRATADA e atualização e manutenção do cadastro dos alunos e professores.

5.8.1 O provimento de conectividade ao Conteúdo Educacional será fornecido pela CONTRATADA e estará limitado a 3GB por mês por dispositivo ativado.

5.8.2 O Serviço Gerenciado de Acesso Remoto a Conteúdo Educacional deve garantir que a conectividade dos alunos seja provida pela melhor operadora de cada localidade com a melhor qualidade de banda.

5.8.3 O Serviço Gerenciado de Acesso Remoto a Conteúdo Educacional deve permitir a gestão de utilização dos acessos de dados fornecidos aos alunos e dos Dispositivos de Acesso.

5.8.4 O Serviço de Gerenciado de Acesso Remoto a Conteúdo Educacional deve permitir q realização da mudança do provedor de conectividade ou da operadora de telefonia de forma remota (sem troca do chip);

5.8.5 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 da Secretaria.

5.8.6 A CONTRATADA deve considerar um volume de substituição do provedor de conectividade ou da operadora móvel a ser realizada pela CONTRATADA em até 15% do total de usuários ativos na base da CONTRATANTE.

5.8.7 O Serviço Gerenciado de Acesso Remoto a Conteúdo Educacional deve possuir Service Desk para atendimento aos colaboradores da Secretaria da Educação envolvidos no projeto. O Service Desk deve tirar dúvidas e auxiliar o colaborador em processos relacionados ao projeto.

5.8.8 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 pela Secretaria da Educação para gestão da plataforma.

5.8.9 Para o Serviço Gerenciado de Acesso a Conteúdo Educacional a CONTRATADA deverá manter durante toda vigência do contrato pessoa devidamente treinada na plataforma, esta pessoa deve ser alocada dentro da Secretaria de Educação auxiliando os colaboradores da Secretaria no que for necessário para a melhor utilização da plataforma.

6. DETALHAMENTO DOS SERVIÇOS

6.1 A CONTRATADA deve possuir equipe para realizar manutenção dos Dispositivos de Acesso e spare parts para realizar troca de componentes sempre que necessário. Além disso, deve manter em estoque mínimo de 5% do total de equipamentos ativados para trocas exigidas pelo projeto.

6.2 A CONTRATADA será responsável pela conexão LAN TO LAN entre as estruturas das operadoras de telefonia móvel e o Data Center onde a Solução de Gestão e Controle dos Acessos e Conectividade for instalada.

6.3 A conexão LAN TO LAN deve estar adequada à necessidade de acessos simultâneos totais por turno manhã, tarde e noite.

6.4 É de responsabilidade da CONTRATADA possuir equipe capacitada para desenvolver, parametrizar, customizar e manter a plataforma tecnológica e toda infraestrutura funcional dentro dos padrões e níveis de serviço exigidos neste Termo de Referência e seus anexos.

6.5 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.

6.6 A CONTRATADA deve disponibilizar analista de suporte alocado na Secretaria de Educação (de segunda a sexta-feira, no mínimo 8 horas diárias, 40 horas semanais) exclusivo para gerir os componentes da solução e auxiliar os responsáveis do projeto dentro da Secretaria da Educação.

6.7 Quando do fornecimento dos aplicativos móveis e aplicações a serem utilizados pelos colaboradores da CONTRATANTE, a instalação será de responsabilidade da CONTRATANTE.

6.8 A CONTRATANTE ficará responsável pela definição da lista de sites ou portais de conteúdos liberados.

6.9 A Solução de Gestão e Controle dos Acessos e Conectividade será realizada pela CONTRATADA, devendo esta prestar o serviço com melhor cobertura em cada localidade.

6.10 É de responsabilidade da CONTRATADA a realização de assistência técnica corretiva de todos os componentes da solução.

6.11 A CONTRATADA deve disponibilizar acesso online aos relatórios de atendimentos corretivos.

6.12 É de responsabilidade da CONTRATADA executar atividades de programação, manutenção preventiva e corretiva da plataforma tecnológica, garantindo o cumprimento das normas e níveis de serviços. Tais atividades são:

6.12.1 Identificar e corrigir falhas na plataforma;

6.12.2 Executar alterações de configurações;

6.12.3 Instalar, configurar e manter softwares da solução;

6.12.4 Monitorar o serviço e sistema;

6.12.5 Fazer backup das configurações do sistema;

6.12.6 Verificar redundância e failover do sistema;

6.12.7 Fazer checklist diário do funcionamento da plataforma;

6.12.8 Executar rotina de testes;

6.12.9 Verificar logs;

6.12.10 Testar conexões;

6.12.11 Avaliar interfaces dos Dispositivos de Acesso;

6.12.12 Avaliar as condições de funcionamento do sistema.

6.13 A CONTRATADA deve comprovar proficiência do analista de suporte na plataforma tecnológica a ser gerenciada por ele.

6.14 A CONTRATADA deve disponibilizar atendimento em conformidade com o nível de serviço informado neste Termo de Referência.

6.15 Durante o período de implantação e ativação de Solução de Gestão e Controle dos Acessos e Conectividade, a CONTRATADA deve fornecer apoio à ativação disponibilizando:

6.15.1 1 pessoa na Secretaria da Educação com conhecimento na plataforma e no processo de ativação. O analista de suporte técnico a ser alocado durante a vigência do contrato por ser a pessoa responsável pela etapa de implantação;

6.15.2 Service Desk com atendimento via telefone, email e/ou chat em horário compatível com funcionamento das escolas.

7. ACORDO DO NÍVEL DE SERVIÇO

7.1 Todo o cronograma de implantação deve ser apresentado a Secretaria de Educação e Inovação, com antecedência mínima de 05 (cinco) dias úteis, para análise e aprovação antes do início da implantação.

7.2 A execução dos serviços não deve exceder os prazos descritos:

7.2.1 Serviço de Capacitação de Professores em "Aula Interativa": até 30 (trinta) dias corridos da assinatura do contrato

7.2.2 Implantação e Ativação da Solução de Gestão e Controle dos Acessos e Conectividade: até 60 (sessenta) dias corridos da assinatura do contrato.

7.2.3 Fornecimento dos Dispositivos de Acesso em endereço definido pela Secretaria da Educação: até 60 (sessenta) dias corridos após assinatura do contrato.

7.2.4 Ativação dos dispositivos: até 30 (trinta) dias corridos após fornecimento dos Dispositivos de Acesso e da Implantação e Ativação da Solução de Gestão e Controle dos Acessos e Conectividade.

7.3 Para os Serviços Gerenciado de Acesso Remoto a Conteúdo Educacional a CONTRATADA deve atender aos prazos de atendimento de acordo com 03 (três) níveis de criticidade:

7.3.1 Alta: Mais de 10% de todos os recursos ou data center inoperante, usuários sem acesso ao Serviço Gerenciado de Acesso Remoto a Conteúdo Educacional;

7.3.2 Média: Menos de 10% dos recursos inoperantes e/ou funções importantes indisponíveis;

7.3.3 Baixa: Situações que afetem apenas usuários específicos nunca superando 5% dos usuários.

7.4 Para o caso de Dispositivos de Acesso com defeitos a CONTRATADA deve realizar o envio de novo equipamento em até 72 horas após solicitação da CONTRATANTE.

7.5 Para os casos de dispositivos com defeito devido a mau uso a CONTRADA deverá realizar diagnóstico e efetuar cobrança à CONTRATANTE no valor de um novo dispositivo, conforme preço de mercado no momento do ocorrido.

7.6 O serviço objeto desta contratação deve ser prestado 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.

7.7 O serviço deve ser realizado de forma ininterrupta, com disponibilidade anual mínima em 98% (noventa e oito por cento) do tempo contratado.

7.8 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.

8. DO SUPORTE TÉCNICO

8.1 A CONTRATADA deve prestar serviços de suporte técnico especializado de forma contínua durante toda a vigência do contrato, objetivando a orientação da Secretaria de Educação e Inovação quanto às ações necessárias para o uso dos recursos oferecidos pela plataforma.

8.2 Deve ser disponibilizada pela CONTRATADA um serviço de abertura de chamados técnicos (Service Desk) através da WEB, 0800 ou número local. Estes serviços são para uso exclusivo dos responsáveis da CONTRATANTE e deverão estar disponíveis de segunda à sexta-feira das 8h às 18h, exceto feriados.

8.3 Ambas as opções fornecidas no serviço de abertura de chamados devem permitir o registro da data e hora da solicitação, o usuário, a descrição do problema e uma numeração de controle.

8.4 Ao final de cada atendimento realizado, deve ser mantido registro com no mínimo as seguintes opções:

8.4.1 Número do chamado;

8.4.2 Data e hora no início do atendimento;

8.4.3 Data e hora no término do atendimento;

8.4.4 Identificação do problema;

8.4.5 Solução aplicada.

8.5 As atividades mínimas contempladas no serviço do atendimento e do analista de suporte são:

8.5.1 Abrir e acompanhar o encerramento dos chamados técnicos;

8.5.2 Realizar atendimento das requisições;

8.5.3 Classificar as requisições;

8.5.4 Identificar prioridades;

8.5.5 Acionar equipe técnica;

8.5.6 Monitorar e garantir nível de serviço contratado;

8.5.7 Realizar manutenção corretiva e preventiva da Plataforma de Gerenciamento;

8.5.8 Gerenciar mudanças no projeto;

8.5.9 Realizar a programação e configuração da solução;

8.5.10 Instalar e configurar aplicativos relacionados ao gerenciamento da plataforma;

8.5.11 Executar rotinas de testes;

8.5.12 Verificar logs;

8.5.13 Elaborar relatórios gerenciais;

8.5.14 Mapear problemas potenciais.

8.6 O sistema de chamados deve permitir a geração de relatórios referentes a:

8.6.1 Números de chamados abertos em um determinado período;

8.6.2 Número de chamados finalizados em um determinado período;

8.6.3 Tempo médio de finalização de chamados;

8.6.4 Tempo médio de finalização de chamados por tipo de serviço;

8.6.5 Ranking de chamados abertos por usuários.

9. COMPROVAÇÃO RELATIVA À QUALIFICAÇÃO TÉCNICA

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:

- Locação de equipamentos eletrônicos ou dispositivos móveis que possuam comunicação ou transmissão de dados via rede de telefonia móvel: mínimo de 500 (quinhentos) equipamentos simultâneos, por período mínimo de 12 (doze) meses.
- Prestação de serviços de suporte técnico remoto (via central de atendimento) e presencial (via equipe própria de campo), para um parque instalado de 500 (quinhentos) equipamentos simultaneamente, por um período mínimo de 12 (doze) meses;
- Desenvolvimento e disponibilização de aplicativos (softwares) customizados para ambiente WEB e Mobile, hospedados em data center com infraestrutura de TIC de alta disponibilidade;
- 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.

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.

10. DA APRESENTAÇÃO DA PROPOSTA TÉCNICA

10.1 A licitante deverá apresentar junto aos Documentos de Habilitação a documentação técnica da solução ofertada que permita à Contratante verificar o atendimento aos requisitos técnicos contidos neste Termo de Referência.

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

10.2.1 Dispositivo de Acesso

10.2.2 Para a Solução de Gestão e Controle dos Acessos e Conectividade deve apresentar no mínimo catálagos e datasheets das seguintes soluções:

10.2.2.1 Solução de Firewall

10.2.2.2 Solução de Balanceamento de Carga

10.2.3 Data Center Tier III

10.3 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.

11. TESTE DE HOMOLOGAÇÃO

11.1 A LICITANTE provisoriamente colocada em primeiro lugar será convocada pela Pregoeira a participar de teste de homologação da solução proposta, nos moldes descritos no ANEXO II deste Edital.

11.2 A CONTRATANTE exigirá um teste de homologação da solução proposta, que consiste na comprovação de algumas funcionalidades descritas nas especificações do ANEXOS I por meio da etapa de ambiente de testes.

11.3 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.

11.4 Ambiente de Testes

11.4.1 A LICITANTE mais bem classificada em preço será convocada para, em até 5 (cinco) dias úteis, participar de reunião inaugural na Secretaria de Educação e Inovação 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 pelo pregoeiro.

11.4.2 No dia imediatamente posterior à reunião inaugural começa a contagem do prazo máximo de 10 (dez) dias úteis para a LICITANTE apresentar, instalar e configurar as amostras para execução do teste de aceitação pela CONTRATANTE.

11.4.3 O prazo acima poderá ser excepcionalmente prorrogado, a critério da CONTRATANTE, por até 5 (cinco) dias úteis, visando a permitir a realização de eventuais ajustes necessários ao funcionamento da solução.

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

11.4.5 As amostras a serem fornecidas e os testes que deverão ser realizados encontram-se previstos no ANEXO II.

11.4.6 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 e Inovação.

11.4.7 Outras hipóteses de substituição dos modelos e marcas dos equipamentos ofertados deverão ser apresentadas à CONTRATANTE, que analisará a possibilidade de permuta dos itens.

11.4.8 A LICITANTE deve apresentar ao menos um profissional, com conhecimento da solução e dos equipamentos ofertados, para acompanhar e orientar a avaliação da solução.

11.4.9 As amostras serão examinadas e avaliadas pelos servidores do Departamento de TI da Secretaria de Educação e Inovação, e terão o prazo de até 2 (dois) dias úteis para conclusão dos testes.

11.4.10 O prazo acima poderá ser excepcionalmente prorrogado, a critério da Secretaria de Educação, por até 3 (três) dias úteis, visando a permitir a realização de testes mais detalhados que a equipe técnica entender necessários.

11.5 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.

11.6 Durante a homologação da solução proposta, os demais participantes não poderão interferir ou prejudicar a realização dos testes.

11.7 Todas as despesas e providências decorrentes do teste, 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 à Secretaria da Educação e Inovação.

11.8 A recusa em providenciar os testes, bem como a não aceitação justificada da solução pela Secretaria de Educação e Inovação, mediante relatório técnico, acarretará a desclassificação da LICITANTE.

A Pregoeira informará a data e a hora em que será divulgado o resultado da verificação do ambiente de teste e será dado prosseguimento à sessão do pregão.

11.9 Será emitido um relatório sucinto descrevendo os exames realizados e contendo a aprovação ou não dos testes.

11.10 Em caso de desclassificação da LICITANTE, os equipamentos utilizados deverão ser recolhidos em até 5 (cinco) dias úteis contados da divulgação da desclassificação.

12. DO TREINAMENTO PARA UTILIZAÇÃO DO SISTEMA

12.1 Iniciada a implantação da solução, a CONTRATADA deve realizar treinamento inicial para os gestores que forem indicados pela Secretaria de Educação.

12.2 O treinamento inicial tem como objetivo introduzir as funcionalidades da solução, apresentando o fluxo de navegação e tutoriais com informações necessárias para a utilização das funções liberadas para os gestores da secretaria.

12.3 Treinamento será feito de forma remota, em salas de videoconferência em horário comercial.

12.4 Todos os recursos das salas de videoconferência para realização do treinamento são de responsabilidade da CONTRATADA.

12.5 Para melhor aproveitamento e agilidade dos treinamentos, será permitido à formação de turmas com no máximo 40 (quarenta) pessoas.

12.6 Todos os treinamentos deverão ser ministrados por profissionais capacitados da CONTRATADA.

12.7 Cada representante escolhido pela CONTRATANTE para realizar o treinamento deve receber explicações teóricas e demonstrações práticas.

12.8 O treinamento deve ser realizado em até 8 horas e a CONTRATADA devem manter plataforma EAD com os cursos disponíveis aos colaboradores da CONTRATANTE.

12.9 Deve ser fornecido material didático digital pela CONTRATANTE.

13. DAS OBRIGAÇÕES

13.1 Obrigações da CONTRATANTE

13.1.1 A CONTRATANTE deve ser responsável pela definição da lista de conteúdos que farão parte da lista de endereços web liberados.

13.1.2 Solicitar a execução do objeto à CONTRATADA através da emissão de Ordem de Serviço.

13.1.3 Tomar todas as providências necessárias ao fiel cumprimento das cláusulas deste Termo de Referência.

13.1.4 Franquear à CONTRATADA o acesso livre à sua instalação sempre que necessário à prestação do serviço.

13.1.5 Facilitar por todos os meios o cumprimento da execução do contrato, dando acesso e promovendo o bom entendimento entre seus funcionários e colaboradores da CONTRATADA, cumprindo com as obrigações pré-estabelecidas.

13.1.6 Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA.

13.1.7 Notificar a CONTRATADA de qualquer irregularidade decorrente da execução do objeto contratual.

13.1.8 Efetuar os pagamentos devidos à CONTRATADA nas condições estabelecidas neste Termo.

13.1.9 Fornecer à CONTRATADA, informações e especificações indispensáveis para a realização dos trabalhos.

13.1.10 Viabilizar a capacitação de pessoal para assegurar o melhor uso das ferramentas.

13.1.11 Analisar as questões relacionadas com o desenvolvimento e operacionalização dos serviços prestados identificando eventuais problemas, diagnosticando-os e propondo medidas preventivas e corretivas.

13.1.12 Nomear através de portaria um Gestor de Contrato com conhecimento em TI para as etapas de verificação e aceitação das amostras dos produtos ofertados.

13.2 Obrigações da CONTRATADA

13.2.1 A CONTRATADA será a responsável pelo fornecimento de todos os serviços e recursos especificados nos itens e subitens do Termo de Referência e seus anexos, a qual será devidamente formalizada a partir de instrumentos contratuais específicos, conforme Edital e seus anexo.

13.2.2 Atender a todas as condições de habilitação e qualificação exigidas na licitação.

13.2.3 Dar suporte à CONTRATANTE na realização de todas as fases de implementação do serviço.

13.2.4 Dimensionar e alocar, as suas expensas, os recursos materiais e humanos necessários para prestação do serviço.

13.2.5 Responsabilizar-se pelos serviços previstos nesse instrumento.

13.2.6 Prestar serviço de manutenção corretiva, que consistirá no fornecimento de novas versões para correção de erros e bugs, e para adaptações em decorrência de evoluções tecnológicas.

13.2.7 Cumprir os prazos e condições dispostos no Acordo de Nível de Serviço e nos prazos estabelecidos nesse instrumento.

14. PARTICIPAÇÃO DAS EMPRESAS EM CONSÓRCIO

14.1 É PERMITIDA a participação de empresas em consórcio, devendo ser observadas as seguintes normas.

14.1.1 Indicação de empresa responsável pelo consórcio (líder), conferindo-lhes amplos poderes para representar os consorciados no procedimento licitatório e no instrumento contratual, receber e dar quitação, responder administrativa e judicialmente, inclusive receber notificação, intimação e citação.

14.1.2 Comprovação do compromisso público ou particular de constituição do consórcio, com a indicação do seu nome, assinado pelas consorciadas, contendo a indicação da empresa líder perante a Secretaria de Educação, pelos atos realizados pelo consórcio, sem prejuízo da responsabilidade solidária das empresas consorciadas deverá ter as seguintes responsabilidades explícitas:

14.1.2.1 Compromissos e obrigações das consorciadas, dentre os quais o de que cada consorciada responderá, individual e solidariamente, pelas exigências de ordens fiscais, administrativas e contratuais pertinentes ao objeto, até a conclusão dos trabalhos e serviços do certame;

14.1.2.2 Declaração expressa de responsabilidade solidária, ativa e passiva, das consorciadas pelos atos praticados pelo consórcio, em relação à licitação e, posteriormente, ao eventual contrato, até o final da execução;

14.1.2.3 Compromisso de não alteração da composição do consórcio ou constituição sob qualquer forma, até o final do contrato;

14.1.2.4 Compromisso expresso de que o consórcio não se constitui, nem se constituirá em pessoa jurídica distinta de seus membros, nem terá denominação própria ou diferente de suas consorciadas;

14.1.2.5 Compromisso e a divisão do escopo no fornecimento para cada uma das consorciadas, individualmente, em relação ao objeto, bem como percentual de participação de cada uma em relação ao objeto, bem como o percentual de participação de cada uma em relação ao custo do fornecimento dos serviços;

14.1.2.6 Previsão de que os pagamentos poderão ser feitos diretamente à empresa consorciada executora da atividade ou a empresa líder.

14.1.3 Apresentação dos documentos exigidos para habilitação por parte de cada consorciado, admitindo-se, para efeito de qualificação técnica, o somatório dos quantitativos de cada consorciado, e, para efeito de qualificação econômico-financeira, o somatório dos valores de cada consorciado, na proporção de sua respectiva participação.

14.1.4 No consórcio de empresas brasileiras com empresas estrangeiras, a liderança caberá, obrigatoriamente, a uma empresa brasileira, sendo que um consórcio, se vencedor, fica obrigado a promover, antes da celebração do contrato, a constituição e o seu registro.

14.1.5 O licitante vencedor fica obrigado a promover, antes da celebração do contrato, a constituição e registro do consórcio.

14.2 Da Justificativa da Participação do Consórcio

14.2.1 Os serviços objeto desta licitação em questão, pela sua complexidade e características multifuncional, não poderiam ser licitados de forma restritiva.

14.2.2 A restrição à participação de consórcio em serviços cujo objeto é complexo e de características multifuncional contraria os interesses da administração pública em suas contratações e afasta empresas plenamente capazes da concorrência em total desalinho com os princípios, em especial o que garante que deve ser buscada a seleção da proposta mais vantajosa.

14.2.3 O objeto da licitação supracitada possui itens heterogêneos que necessitam de total integração entre si, para isso, é fundamental total sinergia e conhecimento do projeto pela equipe de implantação inviabilizando o parcelamento material do objeto licitado.

14.2.4 Dessa forma permitir a participação de mais de uma empresa na elaboração dos serviços, além do reforço de capacidade técnica e financeira do licitante, proporciona maior disponibilidade a equipamento e pessoal especializado, podendo comportar a participação de maior número de empresas visando aumentar a competividade.

14.2.5 É imperativo observar que ao permitir o consórcio há um aumento da participação dos concorrentes, permitindo que empresas que não poderiam participar isoladamente do certame o fizesse por meio de consórcio, assim a Administração Pública amplia de forma direta e ampla a competividade em busca da melhor proposta. Um consórcio é uma das formas de ampliações do universo de proponentes, sobretudo com objetivos voluptuosos e de maior complexidade técnica e financeira, sendo mais do que uma faculdade posta à disposição, consistindo, verdadeiramente, um legítimo dever-poder a ser seguido em razão do interesse público.

14.2.6 Além disso, no Brasil, serviços de natureza semelhantes aos do objeto apresentado vem sendo executadas em regime de consórcio, assim como os seus respectivos gerenciamentos /fiscalizações, não resultando qualquer prejuízo à Administração Pública, mas sim aumentando a garantia de efetividade nas contratações. É cediço, ademais, que não há risco em se contratar em consórcio sob nenhum aspecto, eis que do consórcio surge a responsabilidade solidária pelos atos praticados. Assim, não há risco e nem prejuízo à Administração.

14.2.7 Ademais, a complexidade, envergadura e multidisciplinaridade dos serviços licitados deveriam permitir a possibilidade de participação em consórcio para o melhor atendimento do objeto licitado, bem como a boa execução do contrato. É cediço lembrar que a previsão legal para a formação de consórcios ajuda a facilitar a competição diante do reduzido número de empresas com condições de participar nas licitações de grande complexidade, evitando a reserva de mercado.

15. PRAZOS DE VIGÊNCIA DO CONTRATO

15.1 A licitante vencedora terá o prazo máximo de 05 (cinco) dias úteis, a contar do recebimento da convocação da CONTRATANTE, para assinatura da Ata de Registro de Preços;

15.2 A empresa detentora da ata de registro de preços terá o prazo máximo de 05 (cinco) dias úteis, a contar do recebimento da convocação do órgão CONTRATANTE, para assinatura do contrato;

15.3 A CONTRATADA deverá prestar os serviços pelo prazo de 12 (doze) meses. O contrato poderá ser prorrogado em conformidade com a Lei Federal 8.666/93, de 21/06/1993.

15.4 Os preços previstos para a contratação do objeto deste Contrato permanecerão fixos e irreajustáveis pelo período de 12 (doze) meses. Decorrido esse prazo, os preços poderão ser reajustados com base na variação do Índice Nacional de Preços ao Consumidor Amplo – IPCA, do Instituto Brasileiro de Geografia e Estatística – IBGE, sendo aplicado o índice do mês anterior ao reajuste;

15.5 Quando o participante vencedor não assinar a Ata de Registro de Preços, é facultada a CONTRATANTE convocar os participantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições, ou revogar a licitação, sem prejuízo das sanções previstas neste Termo de Referência e no art. 7º da Lei Federal 10.520/2002, observada a ampla defesa e o contraditório;

15.6 A Ata de Registro de Preços resultante deste certame terá vigência de 12 (doze) meses contados a partir de sua assinatura, obrigando-se a CONTRATADA a garantir o objeto e os preços ajustados;

15.7 Os preços serão fixos durante a vigência da Ata de Registro de preços;

15.8 O contrato terá vigência de 12 (doze) meses a contar da data de sua assinatura, prorrogada por iguais e sucessivos períodos com vistas à obtenção de preços e condições mais vantajosas para a administração, limitada a 60 (sessenta) meses;

15.9 Fica assegurado o restabelecimento do equilíbrio econômico-financeiro inicial do contrato, na ocorrência de fato superveniente que implique a inviabilidade de sua execução.

16. DO VALOR DA CONTRATAÇÃO

16.1 O valor máximo estimado para a contratação da prestação dos serviços será de R$**..... (.....)** mensal, perfazendo um valor máximo estimado anual de R$.....(.....).

17. DA FORMA DE PAGAMENTO

17.1 O pagamento pelos serviços prestados será efetuado em moeda brasileira (real) através de depósito bancário, em conta corrente da empresa contratada, em até 30 (trinta) dias dos efetivos serviços prestados, mediante atesto da nota fiscal pelo departamento responsável pela fiscalização dos serviços.

17.2 Devendo estar inclusos nos preços preços, todos e quaisquer tributos, sejam eles fiscais, sociais,trabalhistas, previdenciários, comerciais ou de qualquer outra natureza resultantes da execução do contrato.

17.3 A contratante reserva-se o direito de suspender o pagamento se os serviços prestados se configurarem em desacordo com as condições e especificações constantes neste Termo de Referencia, no edital e seus anexos.

17.4 O pagamento fica condicionado a comprovação de que a contratada encontra-se adimplente com a fazenda publica federal, estadual e municipal,

FGTS e débitos trabalhistas. A nota fiscal deverá ser preenchida com a indicação do banco, agência e conta corrente para o respectivo deposito.

18. DO CRITÉRIO DE JULGAMENTO

18.1 O critério de julgamento do certame será o menor preço global.

19. DOS RECURSOS FINANCEIROS

19.1 DOTAÇÃO ORÇAMENTÁRIA

19.2 ELEMENTO DE DESPESAS

José Fernando Veloso Monteiro
Secretário de Educação e Inovação
Portaria nº 016/2021

ANEXO I

REQUISITOS TÉCNICOS DO DISPOSITIVO DE ACESSO

O Dispositivo de Acesso fornecido pela CONTRATADA deve realizar a conexão à internet por meio das redes móveis (3G ou 4G) de todas as operadoras disponíveis nas localidades, priorizando sempre a operadora com melhor conectividade.

O dispositivo fornecido deve conectar o tablet, notebook ou smartphone do aluno à internet por meio de uma rede wi-fi criada pelo equipamento. O aluno terá acesso a uma rede por meio de login e senha.

O Dispositivo de Acesso 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.
8.11.21.

REQUISITOS DA SOLUÇÃO DE GESTÃO E CONTROLE DOS ACESSOS E CONECTIVIDADE

A Solução de Gestão e Controle dos Acessos e Conectividade fornecida pela CONTRATADA deve possuir capacidade para no mínimo 6.757 acessos simultâneos o que representa 100% dos alunos e professores conectados simultaneamente aos servidores de conteúdo disponibilizados pela Secretaria de Educação para a educação remota. Possuindo no mínimo 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 (e)SIM 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:

5.1 Solução de Firewall de Próxima Geração

5.2 Solução de Balanceamento de Carga

5.3 Solução de Armazenamento de Logs e Relatórios

As especificações mínimas de cada solução são descritas abaixo:

5.1 Solução de Firewall

5.1 A Solução de Firewall instalado no Data Center da CONTRATADA deve ser composto por hardware e software.

5.2 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.

5.3 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.

5.4 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

5.5 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.

5.6 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada

5.7 A Solução de Firewall deve possuir no mínimo as seguintes características:

5.7.1 Throughput de, no mínimo, 140 Gbps com a funcionalidade de firewall habilitada, independentemente do tamanho do pacote.

5.7.2 Suporte a, no mínimo, 12.000.000 conexões simultâneas.

5.7.3 Suporte a, no mínimo, 700.000 novas conexões por segundo.

5.7.4 Throughput de, no mínimo, 50 Gbps de VPN IPSec.

5.7.5 Deve estar licenciado para, ou suportar sem o uso de licença, 15.000 túneis de VPN IPSEC Site-to-Site simultâneos.

5.7.6 Deve estar licenciado para, ou suportar sem o uso de licença, 80.000 túneis de clientes VPN IPSEC simultâneos.

5.7.7 Throughput de, no mínimo, 10 Gbps de VPN SSL.

5.7.8 Suporte a, no mínimo, 5000 clientes de VPN SSL simultâneos.

5.7.9 Suportar no mínimo 12 Gbps de throughput de IPS.

5.7.10 Suporte a, no mínimo, 30 Gbps de throughput de Application Control.

5.7.11 Suportar no mínimo 15 Gbps de throughput de Inspeção SSL.

5.7.12 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.

5.7.13 Caso o fabricante escolhido pela CONTRATADA divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.
5.7.14 Deve possuir ao menos 2 interfaces 10 GE SFP+.
5.7.15 Deve possuir ao menos 16 interfaces 1 GE RJ-45.
5.7.16 Deve possuir ao menos 8 interfaces 1 GE SFP.
5.7.17 Deve possuir ao menos 12 interfaces 25GE SFP28.
5.7.18 Deve possuir ao memos 4 interfaces 40GE QSFP+.
5.7.19 Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance.
5.8 O equipamento de firewall deve possuir alimentação Dual / tensão de 100-240 VAC.
5.9 O equipamento de firewall deve possuir alimentação Dual / frequência de 50/60 Hz.
5.10 O equipamento de firewall deve possuir deve possuir fonte de alimentação redundante que permitam troca a quente e caso de defeito.
5.11 O equipamento de firewall deve possuir temperatura - faixa de operação de 0º a 40º C.
5.12 O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.
5.13 Os dispositivos de proteção de rede devem possuir:
5.13.1 suporte a 4094 VLAN Tags 802.1q.
5.13.2 suporte a Policy based routing ou policy based forwarding.
5.13.3 suporte a roteamento multicast (PIM-SM e PIM-DM).
5.13.4 suporte a DHCP Relay.
5.13.5 suporte a DHCP Server.
5.13.6 suporte a Jumbo Frames.
5.14 Os dispositivos de proteção de rede devem suportar:
5.14.1 sub-interfaces ethernet logicas.
5.14.2 NAT dinâmico (Many-to-Many).
5.14.3 NAT estático (1-to-1).
5.14.4 NAT estático bidirecional 1-to-1.
5.14.5 Tradução de porta (PAT).
5.14.6 NAT de Origem.
5.14.7 NAT de Destino.
5.14.8 NAT de Origem e NAT de Destino simultaneamente.
5.15 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
5.16 Deve suportar NAT64 e NAT46.
5.17 Deve implementar o protocolo ECMP.
5.18 Deve implementar balanceamento de link por hash do IP de origem.
5.19 Deve implementar balanceamento de link por hash do IP de origem e destino.

5.20 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.
5.21 Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais.
5.22 A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação.
5.23 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.
5.24 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.
5.25 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.
5.26 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).
5.27 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.
5.28 Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de roteamento.
5.29 Deve permitir monitorar via SNMP falhas de hardware, monitoramento de CPU e memória, de segurança e interface.
5.30 Deve enviar log para sistemas de monitoração externos, simultaneamente.
5.31 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL.
5.32 Deve possuir proteção anti-spoofing.
5.33 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).
5.34 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).
5.35 Deve suportar OSPF graceful restart.
5.36 Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.
5.37 Deve suportar Modo Camada 2 (L2), para inspeção de dados em linha e visibilidade do tráfego.
5.38 Deve suportar Modo Camada 3 (L3), para inspeção de dados em linha visibilidade do tráfego.
5.39 Deve suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente.
5.40 Deve suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3.
5.41 Deve suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster.
5.42 Deve realizar configuração em alta disponibilidade deve sincronizar: Sessões.

5.43 A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede.
5.44 A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs.
5.45 A configuração em alta disponibilidade deve sincronizar:Tabelas FIB.
5.46 O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
5.47 Deve possuir suporte a criação de sistemas virtuais no mesmo appliance.
5.48 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.
5.49 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.
5.50 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).
5.51 Controle por Política de Firewall.
5.52 Deve suportar controles por zona de segurança.
5.53 Deve possuir controles de políticas por porta e protocolo.
5.54 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.
5.55 Deve possuir controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
5.56 Deve possuir controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).
5.57 Deve possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
5.58 Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound).
5.59 Deve descriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2.
5.60 Deve possuir controle de inspeção e descriptografia de SSH por política.
5.61 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.
5.62 Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo).
5.63 QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
5.64 Deve ter suporte a objetos e regras IPV6.
5.65 Deve ter suporte a objetos e regras multicast.
5.66 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.

5.67 Deve suportar atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

5.68 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

5.69 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

5.70 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.

5.71 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.

5.72 Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.

5.73 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.

5.74 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.

5.75 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.

5.76 Deve identificar o uso de táticas evasivas via comunicações criptografadas.

5.77 Atualizar a base de assinaturas de aplicações automaticamente.

5.78 Deve permitir a limitação da banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos.

5.79 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.

5.80 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.

5.81 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.
5.82 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.
5.83 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.
5.84 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.
5.85 A solução utilizada pela CONTRATADA deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.
5.86 Deve alertar o usuário quando uma aplicação for bloqueada.
5.87 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos.
5.88 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos.
5.89 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo.
5.90 Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos.
5.91 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).
5.92 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação.
5.93 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.
5.94 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.
5.95 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).
5.96 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.
5.97 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade.

5.98 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.
5.99 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.
5.100 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.
5.101 Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.
5.102 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.
5.103 Deve permitir o bloqueio de vulnerabilidades.
5.104 Deve permitir o bloqueio de exploits conhecidos.
5.105 Deve incluir proteção contra-ataques de negação de serviços.
5.106 Deve possuir o seguinte mecanismo de inspeção de IPS:
5.106.1 Análise de padrões de estado de conexões.
5.106.2 Análise de decodificação de protocolo.
5.106.3 Análise para detecção de anomalias de protocolo.
5.106.4 Análise heurística.
5.106.5 IP Defragmentation.
5.106.6 Remontagem de pacotes de TCP.
5.106.7 Bloqueio de pacotes mal formados.
5.107 Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.
5.108 Deve detectar e bloquear a origem de portscans.
5.109 Deve bloquear ataques efetuados por worms conhecidos.
5.110 Deve possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.
5.111 Deve possuir assinaturas para bloqueio de ataques de buffer overflow.
5.112 Deve possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.
5.113 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.
5.114 Deve permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.
5.115 Deve identificar e bloquear comunicação com botnets.
5.116 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.
5.117 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou por filtro pré-definido.

5.118 Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.
5.119 Os eventos devem identificar o país de onde partiu a ameaça.
5.120 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
5.121 Deve possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
5.122 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.
5.123 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).
5.124 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.
5.125 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.
5.126 Deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.
5.127 Deve possuir pelo menos 60 categorias de URLs.
5.128 Deve possuir a função de exclusão de URLs do bloqueio, por categoria.
5.129 Deve permitir a customização de página de bloqueio.
5.130 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).
5.131 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.
5.132 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.
5.133 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.
5.134 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.

5.135 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
5.136 Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.
5.137 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).
5.138 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.
5.139 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.
5.140 Deve permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução.
5.141 Deve prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.
5.142 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.
5.143 Deve suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem.
5.144 Deve suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino.
5.145 Deve suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo.
5.146 Deve suportar a criação de políticas de QoS e Traffic Shaping por aplicações.
5.147 Deve suportar a criação de políticas de QoS e Traffic Shaping por porta.
5.148 O QoS deve possibilitar a definição de tráfego com banda garantida.
5.149 O QoS deve possibilitar a definição de tráfego com banda máxima.
5.150 O QoS deve possibilitar a definição de fila de prioridade.
5.151 Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
5.152 Suportar marcação de pacotes Diffserv, inclusive por aplicação.
5.153 Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping.
5.154 Deve suportar identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc).
5.155 Deve suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

5.156 Deve suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.
5.157 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.
5.158 Deve suportar a criação de políticas por geolocalização, permitindo o trafego de determinado Pais/Países sejam bloqueados.
5.159 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
5.160 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.
5.161 Deve suportar VPN Site-to-Site e Cliente-To-Site.
5.162 Deve suportar IPSec VPN.
5.163 Deve suportar SSL VPN.
5.164 A VPN IPSEc deve suportar 3DES.
5.165 A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.
5.166 A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.
5.167 A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).
5.168 A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard).
5.169 A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.
5.170 Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
5.171 Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting.
5.172 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.
5.173 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.
5.174 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.
5.175 Atribuição de DNS nos clientes remotos de VPN.
5.176 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.
5.177 Deve suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local.
5.178 Deve suportar leitura e verificação de CRL (certificate revocation list).
5.179 Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.
5.180 Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação.

5.181 Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação.
5.182 Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário.
5.183 Deverá manter uma conexão segura com o portal durante a sessão;
5.184 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).
5.185 Durante a vigência do contrato a CONTRATADA deve manter os softwares sempre atualizados na versão mais recente sem nenhum custo adicional.

6 **Solução de Balanceamento de Carga**

6.1 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:
6.1.1 Throughput mínimo de camada 4 de 40 Gbps.
6.1.2 Throughput mínimo de camada 7 de 25 Gbps.
6.1.3 Deve suportar no mínimo 35 milhões de conexões concorrentes.
6.1.4 Deve possuir aceleração de SSL baseada em hardware.
6.1.5 Deve estar licenciado para no mínimo 30 instâncias virtuais.
6.1.6 Deve possuir ao menos 128 GB de disco.
6.1.7 Deve possuir ao menos 6 interfaces gigabit ethernet RJ-45.
6.1.8 Deve possuir ao menos 6 interfaces gigabit ethernet SFP.
6.1.9 Deve possuir ao menos 4 interfaces 10 gigabit ethernet.
6.2 Deve suportar a criação de contas de administradores com diferentes perfis de acesso e direitos (Role based).
6.3 A solução deve permitir balancear em camada 7 os seguinte protocolos: HTTP, HTTPs, TurboHTTPS, RADIUS, RDP, SIP, TCPs, DNS, SMTP, RTMP, RTSP, MySQL.
6.4 Deve balancear tráfego entre servidores reais usando algoritmos próprios e usado informação de saúde de servidores reais.
6.5 Deve permitir a configuração de perfis que determinem a criptografia do tráfego entre o equipamento e os servidores reais.
6.6 Quando houver comunicação encriptada esta deverá ser controlada por protocolos SSL/TLS e lista de ciphers.
6.7 Deve suportar os protocolos SSL (v2 e v3) e TLS (v1.0, v1.1, v1.2).
6.8 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.
6.9 Deve ser capaz de reutilizar sessões SSL.
6.10 Para cada um dos servidores que participarão do algoritmo de balanceamento deve ser possivel configurar: peso (para fins de controle de preferencia 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).

6.11 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 cabelho de requisição HTTP do cliente, hash de parametro de URL encontrado em requisição HTTP vinda do cliente, atributo de RADIUS.

6.12 Deve ter capacidade de re-escrever o cookie vindo do servidor real para uso em regras de persistência.

6.13 Deve suportar a configuração de timeouts de conexão submetidas a persistência.

6.14 O sistema deve permitir a seleção do servidor real baseado em informação de cabeçalho de pacotes TCP/IP e HTTP.

6.15 Deve possiblitar 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).

6.16 A seleção por campos de cabeçalho HTTP para fins de roteamento deverá ser feita através de expressões regulares ou match completo.

6.17 O sistema deve permitir a reescrita de mensagens de HTTP request, HTTP Response e de cabeçalho HTTP.

6.18 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.

6.19 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.

6.20 O sistema deve possibilitar compressão de dados incluindo: aplicações (java script, SOAP XML, X-javascript, XML) e Texto (CSS, HTML, JavaScript, Plain, XML).

6.21 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:

6.21.1 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.

6.22 O sistema deve possuir perfis de tráfego pre configurados para uso em grupo de servidores reais. Pelo menos os seguintes perfís 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).

6.23 Além dos perfís pre configurados o sistema deve permitir a customização dos perfís 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).

6.24 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;

6.25 Deve implementar NAT, NAT64 e NAT46 (os dois últimos para permitir NAT incluindo IPv4 e IPv6 entre clientes e servidores).

6.26 Deve implementar esquema de autenticação Basic (RFC 2617).

6.27 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.

6.28 Deve possuir mecanismos de balanceamento de tráfego através de vários enlaces de comunicação.

6.29 Deve possibilitar o balanceamento de tráfego inbound (da WAN para a LAN) e outbound (de LAN para a WAN) usando múltiplos enlaces WAN.

6.30 O tráfego a ser balaceado 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.

6.31 Deve possuir mecanismos de persistência de tráfego que ignore algoritmos de balanceamento de tráfego.

6.32 Os mecanismos de persistência devem ser estabelecidos em função de endereços IP destino e origem.

6.33 Deve possuir mecanismos de seleção de rotas em função de latência de tráfego ao destino medido através de ICMP ou TCP echo.

6.34 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.

6.35 Deve ser capaz de estabelecer túneis virtuais com sistemas do mesmo fabricante para transporte de tráfego entre os equipamentos.

6.36 Suporte a estabelecimento de túneis usando encapsulamento GRE (Generic Routing Encapsulation).

6.37 Deve balancear o tráfego entre estes enlaces virtuais baseado em pesos atribuidos aos enlaces ou função de cálculos de hash de endereços IP de origem e destino.

6.38 Suporte a monitoração de estado de saúde de links com ISPs e enlaces virtuais.

6.39 Deve ser possível estabelecer um dos enlaces (virtual ou real) como enlace de backup (usado somente quando primários não estão disponíveis).
6.40 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.
6.41 Deve implementar o protocolo IEEE 802.3ad para balanceamento de tráfego entre portas.
6.42 Deve implementar VLANs e ser compatível com o protocolo IEEE 802.1q.
6.43 Deve permitir o roteamento entre diferentes VLANs.
6.44 Deve suportar a configuração de rotas estáticas incluindo a distância administrativa da mesma para fins de decisão de roteamento de pacotes.
6.45 Deve oferecer suporte a políticas de roteamento baseado em endereços IP de origem e/ou destino.
6.46 Deve suportar OSPF v2 - RFC 2328.
6.47 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).
6.48 Deve fazer alocação de banda passante baseado no trio endereço destino, endereço de origem e serviço (portas TCP e UDP).
6.49 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.
6.50 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.
6.51 Deve suportar implementação em modo transparente, atuando como Bridge L2.
6.52 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).
6.53 Deve possuir funcionalidades de Global Server Load Balancing.
6.54 Deve implementar servidor DNS baseado em versão protegida de BIND versão 9.
6.55 Deve implementar servidor DNS Autoritativo.
6.56 Deve permitir o balaneceamento 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.
6.57 Deve suportar DNSSEC com algoritmo RSASHA1.
6.58 Deve implementar DNS64 para permitir comunicação entre client IPv4 com servidores IPv6 no escopo de balanceamento de carga global.
6.59 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.

6.60 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).

6.61 Deve possibilitar a definição de disponibilidade de serviços através de verificação de saúde em vários protocolos baseados em expressões com AND e OR.

6.62 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.

6.63 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 incluida no sistema.

6.64 A implementação do mecanismo de proximidade de tempo deve ser baseada em ICMP e/ou TCP.

6.65 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.

6.66 Quando implementado como servidor DNS autoritativo deve permitir a configuração de número máximo de respostas fornecidas por segundo.

6.67 Deve permitir a troca de portas HTTP, HTTPS, Telnet e SSH para fins de acesso remoto ao equipamento por parte do administrador.

6.68 Deve suportar a sincronização de horário via NTP.

6.69 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).

6.70 Deve permitir o upgrade através de linha de comendo ou interface gráfica.

6.71 Deve permitir o processo de upgrade em partições distintas.

6.72 Deve suportar o update das 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.

6.73 Deve suportar o update das bases de dados de assinaturas de forma programada indicando dia da semana e hora do dia.

6.74 Deve suportar a configuração de um servidor de email para o envio de emails de alerta.

6.75 Deve implementar o agente de SNMP v1, V2c e 3 (RFC 3414).

6.76 Deve permitir a configuração de eventos SNMP de, pelo menos, níveis de uso de CPU, memória e disco.

6.77 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).
6.78 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).
6.79 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.
6.80 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.
6.81 Deve implementar filtros que possibilitem a visualização de eventos de Administração: indicando ações executadas por administradores.
6.82 Deve implementar filtros que possibilitem a visualização de eventos de Sistema: indicando informações relevantes a operação, avisos e erros gerados pelo sistema.
6.83 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.
6.84 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.
6.85 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.
6.86 Deve implementar filtros que possibilitem a visualização de eventos de Balanceamento de Enlaces: indicando que limite de banda foi atingido; política relacionada ao evento.
6.87 Deve implementar filtros que possibilitem a visualização de eventos de Balanceamento de Carga Global: identificador do servidor real, política relacionada ao evento.
6.88 Deve implementar filtros que possibilitem a visualização de eventos de Firewall: política relacionada ao evento.
6.89 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.

6.90 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.
6.91 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.
6.92 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.
6.93 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.
6.94 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.
6.95 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.
6.96 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.
6.97 Deve ser capaz de armazenar logs no próprio sistema.
6.98 Deve permitir a seleção do menor nível de log a ser gravado localmente.
6.99 Deve permitir a seleção do tipo de log a ser armazenado localmente (Eventos, Segurança e Tráfego) para evitar uso excessivo do disco.
6.100 Deve ser capaz de enviar notificações de logs a servidor syslog.
6.101 Deve permitir a seleção do menor nível de log a ser enviado para o servidor syslog.
6.102 Deve permitir o envio de logs a servidor syslog no formato CSV.
6.103 Deve permitir a seleção do tipo de log a ser enviado ao servidor syslog.
6.104 A solução deve suportar o envio de alertas através de emails, estes alertas podem ser configurados de acordo com a categoria de eventos ou níveis de severidade.
6.105 Deve suportar o envio de alertas através de emails relacionados a pelo menos eventos de: alta disponibilidade, administração, configuração, disco, verificação de saúde, expiração de certificados.
6.106 Deve permitir e emissão de relatorios sob demanda ou programados.
6.107 Deve suportar o envio via email dos relatórios programados em formato PDF.
6.108 Pelo menos os seguintes relatórios devem estar disponíveis no sistema:

6.108.1 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.
6.108.2 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.
6.108.3 DoS: destinos (alvos) mais frequentes com contagem associada.
6.108.4 Geografias: destinos (alvos) mais frequentes com contagem associada, origens mais frequentes com contagem associada, origens mais frequentes com contagem associada e país.
6.108.5 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.
6.109 Deve implementar características de redundância e alta disponibilidade em cluster do mesmo modelo, nos modos ativo-passivo e ativo-ativo.
6.110 A formação do cluster deve permitir a sincronização de configuração e versão de sistema operacional entre os participantes.
6.111 Possuir mecanismos de monitoração de estado de interface que permita a alteração de estado do membro, de ativo para passivo, em caso de falha.
6.112 Os participantes do cluster dever ser do mesmo modelo e ter a mesma versão de sistema operacional.
6.113 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.
6.114 Quando em ativo-passivo apenas um dos membros encaminhará tráfego enquanto que o passivo só encaminhará tráfego caso haja falha no ativo.
6.115 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 intervençao externa ao cluster.
6.116 Na configuração ativo-ativo todos os membros do cluster deverão encaminhar tráfego.
6.117 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.
6.118 Deve permitir a configuração de parâmetro relativo a eleição do sistema primário (aquele em que as configurações são feitas e encaminhadas aos outros membros) dentro do mesmo cluster.
6.119 Se necessário, deve permitir aplicar configurações em qualquer membro do cluster, independentemente se este é primário ou secundário.

6.120 A sincronização da configuração do cluster pode ser realizada através de portas agregados.
6.121 Deve possuir funcionalidades de virtualização, deve possibilitar a implementação de várias instâncias de sistema;
6.122 Deve permitir o provisionamento de diferentes administradores para cada uma das instâncias de sistema.
6.123 A solução deve permitir a encriptação/decriptação de sessões SSL no lugar dos servidores (processo conhecido como SSL Offload).
6.124 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.
6.125 Deve possibilitar a implementação na rede como proxy SSL, neste caso desempenhando papel de proxy para os dois lados da conexão (clientes e servidores).
6.126 Deve suportar pelo menos ciphers: RSA, PFS, ECDHE e eNull para SSL Offload.
6.127 Deve suportar a configuração de ciphers para SSL Offload.

7 Solução de Armazenamento de Logs e Relatórios

7.1 Deve possuir capacidade de receber ao menos 500 GigaBytes de logs diários.
7.2 Não deve possuir limite de utilização de disco.
7.3 Deve suportar acesso via SSH, WEB (HTTPS) e Telnet para o gerenciamento da solução.
7.4 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).
7.5 Permitir acesso simultâneo de administradores permitindo a criação de ao menos 2 (dois) perfis para administração e monitoração.
7.6 Suportar SNMP versão 2 e versão 3 na solução de relatórios.
7.7 Deve permitir a criação de administradores que acessem todas as instâncias de virtualização da solução de relatórios.
7.8 Deve permitir habilitar e desabilitar, para cada interface de rede da solução de relatórios, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet.
7.9 Deve possuir autenticação integrada a servidor Radius.
7.10 Deve permitir a geração de relatórios em tempo real, para a visualização de tráfego observado, nos formatos: mapas geográficos e tabela.
7.11 Deve possuir autenticação integrada ao Microsoft Active Directory.
7.12 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.
7.13 Possuir mecanismo para que logs antigos sejam removidos automaticamente.
7.14 Permitir a importação e exportação de relatórios.
7.15 Deve possuir a capacidade de criar relatórios nos formatos PDF.
7.16 Deve ser possível exportar os logs em CSV.
7.17 Deve gerar logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

7.18 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.
7.19 A solução deve possuir relatórios pré definidos.
7.20 Possuir envio automático de logs para um servidor FTP externo a solução.
7.21 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.
7.22 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.
7.23 Deve possuir a capacidade de personalização de gráficos como barra, linha e tabela para inserção aos relatórios.
7.24 Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em realtime.
7.25 Dever ser possível fazer download dos arquivos de logs recebidos.
7.26 Deve possuir agendamento para gerar e enviar automaticamente relatórios.
7.27 Deve permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades.
7.28 Permitir o envio de maneira automática de relatórios por email.
7.29 Permitir programar a geração de relatórios, conforme calendário definido pelo administrador.
7.30 Deve ser possível definir filtros nos relatórios
7.31 Deve ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros.
7.32 Deve gerar alertas automáticos via Email, SNMP e Syslog baseados em eventos como ocorrência como log, severidade de log, entre outros.
7.33 Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios.
7.34 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.
7.35 Deve permitir ver em tempo real os logs recebidos
7.36 Deve permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino.
7.37 Deve possuir relatório detalhado de prevenção de perda de dados (DLP).
7.38 Deve possuir relatório de VPN.
7.39 Deve possuir relatório de Sistemas de prevenção de intrusão (IPS).
7.40 Deve possuir relatório de reputação do cliente.
7.41 Deve possuir relatório de análise de segurança do usuário.
7.42 Deve possuir relatório de avaliação da ameaça cibernética.

8 Data Center TIER III

O datacenter onde os componentes servidores da solução 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.

8.1 O datacenter deve atender no mínimo as seguintes características:

8.1.1 Deve ser atendido por no mínimo duas empresas de telecomunicações.

8.1.2 Os cabos das empresas de telecomunicação devem vir por rotas distintas até o Data Center.

8.1.3 Deve estar em zonas de proteção contra incêndios.

8.1.4 Possuir sistemas de energia e ar-condicionado distintos.

8.1.5 As conexões entre as salas devem ser feitas via fibra ou pares metálicos redundantes.

8.1.6 Prover pelo menos a redundância elétrica N+1.

8.2 Deve possuir disponibilidade mínima de 99,749% e até 72 horas de proteção contra interrupção de energia.

ANEXO II

DA APRESENTAÇÃO DA AMOSTRA

A Licitante classificada provisoriamente como arrematante da disputa de preços deverá apresentar amostra da solução a ser fornecida, de forma que a Contratante possa certificar a capacidade técnica de fornecimento do objeto licitado.

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.

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

Item a ser verificado	Atendimento às especificações
Documentação técnica da solução apresentada permite verificar o atendimento aos requisitos técnicos exigidos do Termo de Referência.	( ) Atendeu ( ) Não atendeu
Dispositivo de Acesso apresentado é portátil, funciona com bateria e gera rede Wi-Fi protegida por senha e reconhecida por dispositivos tipo Notebook e Smartphone.	( ) Atendeu ( ) Não atendeu
A Licitante deverá apresentar a rede Wi-Fi gerada pelo Dispositivo de Acesso 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 (definida neste momento pela Contratante). A Licitante deverá proceder o cadastro desta URL solicitada na sua ferramenta de controle e liberação de acessos, de forma que o usuário conectado na rede Wi-FI gerada pelo Dispositivo de Acesso passe a conseguir acessar o conteúdo da URL em questão via browser do dispositivo 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 remota do provedor de conectividade ou	( ) Atendeu ( ) Não atendeu

operadora de telefonia móvel do Dispositivo de Acesso, sem a necessidade de substituição no local de componentes previamente instalados. A licitante poderá utilizar na demonstração desta funcionalidade qualquer dispositivo móvel (smartphone ou tablet) que permita apresentar a efetividade do comando remoto para troca de provedor de conectividade ou operadora de telefonia móvel.	
Licitante atendeu todos os requisitos:	( ) Atendeu ( ) Não atendeu

ANEXO III – MODELO DE PROPOSTA DE PREÇOS

A Licitante deve apresentar a proposta de preços em conformidade com a tabela abaixo:

ITEM	DESCRIÇÃO	UNIDADE	QUANT.	PRAZO	PREÇO UNITÁRIO (MENSAL) (R$)	PREÇO TOTAL ANUAL (R$)
1	SERVIÇO DE CAPACITAÇÃO DE PROFESSORES EM "AULA INTERATIVA"	SERVIÇO	700	-		
2	IMPLANTAÇÃO E ATIVAÇÃO DA SOLUÇÃO DE GESTÃO E CONTROLE DOS ACESSOS E CONECTIVIDADE	SERVIÇO	1	-		
3	DISPOSITIVO DE ACESSO	LOCAÇÃO MENSAL	700	12		
4	SERVIÇO GERENCIADO DE ACESSO REMOTO A CONTEÚDO EDUCACIONAL	SERVIÇO MENSAL	8.000	12		
VALOR GLOBAL DA PROPOSTA (12 MESES): R$						