201917249158-1

CONTRATO DE PRESTAÇÃO DE SERVIÇOS
- Serviço de Comunicação Multimídia ("SCM") -

Pelo presente instrumento, de um lado, a **ALGAR MULTIMIDIA S/A**, prestadora de serviços de telecomunicações, inscrita no CNPJ no 04.622.116/0001-13, com sede na Rua Jose Alves Garcia, nº 415, Bairro Brasil, na cidade de Uberlândia, Estado de Minas Gerais, **ALGAR TELECOM S/A**, prestadora de serviços de telecomunicações, inscrita no CNPJ no 71.208.516/0001-74, com sede na Rua Jose Alves Garcia, nº 415, Bairro Brasil, na cidade de Uberlândia, Estado de Minas Gerais e **ALGAR SOLUÇÕES EM TIC S/A**, inscrita no CNPJ sob o nº. 22.166.193/0001-98, Rua José Alves Garcia, 415, Bloco A, Bairro Brasil, Uberlândia/MG, por si ou por suas filiais, e neste ato, por seus representantes, doravante denominadas simplesmente ALGAR TELECOM, e, de outro lado, o CONTRATANTE, conforme identificado no Termo de Contratação, celebram entre si e de comum acordo, o presente Instrumento, nos seguintes termos e condições:

CLÁUSULA PRIMEIRA – DO OBJETO E DAS DEFINIÇÕES

1.1. **DO OBJETO**

O serviço contratado compreende a disponibilização, pela ALGAR TELECOM, dos meios necessários para a prestação dos serviços de comunicação de dados, para o acesso ou a integração à rede Internet, e de serviços adicionais, ambos doravante denominados como ("Serviço(s)").

1.2. **DAS DEFINIÇÕES**:

1.2.1. Para perfeito entendimento e interpretação deste contrato, são adotadas as seguintes definições:

a) CONTRATANTE: Pessoa física ou jurídica que, por si ou seus representantes legais, tenha contratado o SERVIÇO prestado pela ALGAR TELECOM, tornando-se, assim, titular de direitos e sendo responsável pelo cumprimento de todas as obrigações assumidas.

b) PROPOSTA COMERCIAL: é o documento proposto pela ALGAR TELECOM ao CONTRATANTE, indicando preços, prazos, serviço e outros detalhes pertinentes. Salvo se disposto contrário na PROPOSTA COMERCIAL, esta terá prazo de validade de 7 (sete) dias corridos contados da data de sua emissão.

c) TERMO DE CONTRATAÇÃO: é o compromisso pelo qual o CONTRATANTE contrata a um ou outro documento proposto pela ALGAR TELECOM indicando sua plena ciência, concordância e compromisso de obedecer aos termos e condições, incluindo preços e prazos estabelecidos no presente CONTRATO, na Proposta Comercial e/ou Termo de Contratação. A CONTRATAÇÃO poderá ocorrer por qualquer forma admitida em Lei, ainda que eletrônica ou virtual.

d) SERVIÇO DE ATENDIMENTO AO CONTRATANTE: Serviço disponibilizado pela ALGAR TELECOM para atendimento do CONTRATANTE, por meio de atendimento pessoal nas lojas e credenciadas, por meio do *site* www.algartelecom.com.br ou por meio dos telefones 103 12 para a área de concessão da ALGAR TELECOM e 0800 941 2822 para a área de autorização.

e) SERVIÇO: é o conjunto de atividades que, de forma direta ou indireta, possibilita a oferta de serviço de comunicação multimídia ou de serviços adicionais.

f) SOLUÇAO: é o conjunto de SERVIÇOS descritos nos Anexos a este Contrato.

g) CONDIÇAO ESPECIFICA DO SERVIÇO: é o documento vinculado a este Contrato que descreve detalhadamente o SERVIÇO contratado pelo CONTRATANTE.

h) SERVIÇO DE COMUNICACAO MULTIMIDIA: é um serviço fixo de telecomunicações de interesse coletivo, prestado em âmbito nacional e internacional, no regime privado, que possibilita a oferta de capacidade de transmissão, emissão e recepção de informações multimídia (dados, voz e imagem), utilizando quaisquer meios, a usuários dentro de uma área de prestação de serviço.

i) SERVIÇO ADICIONAL: é um serviço acessório que possibilita a disponibilização de uma comodidade ou utilidade ao cliente, indiretamente relacionada com a prestação do serviço de telecomunicações, mas que com esta não se confunde.

1.3. Em caso de divergência entre os documentos mencionados no item 1.1, prevalecerá o disposto na Proposta Comercial e/ou Termo de Contratação.

1.3.1. Em caso de divergência entre os documentos que compõem uma SOLUÇÃO, prevalecerá o específico sobre o genérico.

1.4. Para todos os fins de direito, este documento é parte integrante da Proposta Comercial e Termo de Adesão, produzidos pela ALGAR TELECOM em favor do CONTRATANTE, estando, ainda, disponível para livre consulta no site www.algartelecom.com.br e registrado no Cartório de Registro de Títulos e Documentos e Registro Civil das Pessoas Jurídicas da Comarca de Uberlândia, Estado de Minas Gerais.

CLÁUSULA SEGUNDA –DAS CONDIÇÕES PARA A PRESTAÇÃO DO(s) SERVIÇO(S)

2.1. Como condição para a prestação do SERVIÇO, o CONTRATANTE deverá atender aos requisitos técnicos eventualmente explicitados neste Contrato e Anexos.

2.1.1. Salvo disposição em contrário, será de exclusiva responsabilidade do CONTRATANTE o provimento dos requisitos técnicos, arcando com os riscos e custos a ele inerentes.

2.1.2. Quando o CONTRATANTE utilizar equipamento próprio ou contratado de terceiros que não diretamente o da ALGAR TELECOM, será ele o único responsável pelos custos e necessárias manutenções preventivas/corretivas, bem como as consequências que estes equipamentos causarem direta ou indiretamente aos SERVIÇOS.

2.1.3. Além do disposto no item 2.1, considera-se como condição para a prestação do SERVIÇO a realização de testes da conexão da rede de telecomunicações.

2.2. O SERVIÇO será prestado pela ALGAR TELECOM ou por terceiros, conforme contratado pelo CONTRATANTE, ficando desde já estabelecido que a prestação do SERVIÇO terá início após a assinatura deste Contrato, quando ocorrera a instalação no local de prestação indicado no Termo de Contratação.

2.2.1. O prazo de instalação será aquele indicado no Termo de Contratação.

2.3. Para os SERVIÇOS que se utilizarem, direta ou indiretamente, dos benefícios da Internet, fica desde já registrado que independentemente da ação ou vontade da ALGAR TELECOM, fatores externos podem influenciar diretamente na qualidade/velocidade dos SERVIÇOS.
2.3.1. Por características intrínsecas a Internet, não há garantias quando a origem de dados for originada em rede de terceiros.
2.4. O CONTRATANTE tem ciência que o SERVIÇO poderá ficar, eventualmente, indisponível, seja para manutenção programada (preventiva) ou não programada (emergencial) ou por outros fatores fora do controle da ALGAR TELECOM. Interrupções do SERVIÇO, causadas, comprovadamente, pelo CONTRATANTE ou por eventos de forca maior ou caso fortuito, não constituirão falha no cumprimento das obrigações da ALGAR TELECOM previstas neste contrato.
2.5. Caso o CONTRATANTE se recuse a receber o SERVIÇO e/ou SOLUÇAO, sem justo motivo, após a assinatura do TERMO DE CONTRATAÇÃO, o CONTRATANTE deverá reembolsar todos os custos e/ou investimentos que eventualmente a ALGAR TELECOM tenha realizado, ou pagar uma multa compensatória de 10% (DEZ POR CENTO) calculada sobre o valor total do contrato, o que for maior e a critério da ALGAR TELECOM.

CLÁUSULA TERCEIRA – DO PAGAMENTO, RESPECTIVAS SANÇÕES E CONTESTAÇÃO DE DÉBITOS

3.1 A ALGAR TELECOM notificará o CONTRATANTE acerca da ativação do(s) Serviço(s) por meio eletrônico (*e-mail*) ou presencial com a assinatura do CONTRATANTE na ordem de serviço. A notificação realizada por e-mail será encaminhada para a pessoa indicada na PROPOSTA COMERCIAL e/ou TERMO DE CONTRATAÇÃO. Transcorridos 5 (cinco) dias do recebimento da referida notificação, sem manifestação do CONTRATANTE, a instalação do(s) serviço(s) será considerada aceita pelo CONTRATANTE e ensejará, a partir da data do envio da notificação, o início da prestação do serviço e cobrança do(s) serviço(s) prestado.
3.1.1 Caso o CONTRATANTE se manifeste no prazo mencionado acima, a ALGAR TELECOM deverá avaliar o pleito formulado, e se for o caso, sanar a anomalia do serviço no prazo de 5 (cinco) dias a contar do recebimento da notificação do CONTRATANTE, ensejando, após tal procedimento, o envio de um novo *e-mail* ao CONTRATANTE, na forma do item 3.1.
3.1.2 Caso a ALGAR TELECOM constate que o serviço não apresente qualquer defeito, ou, ainda, que tais defeitos sejam comprovadamente originados de qualquer ação culposa ou dolosa do CONTRATANTE, seus prepostos e/ou seus contratantes finais ou que o atraso na ativação resulte de pendências não sanadas na infraestrutura do CONTRATANTE ou de seu prestador de serviço, a data de entrega e ativação mencionada no item 3.1. será mantida e utilizada para fins deste Contrato, especialmente no que se refere a cobrança e contagem do prazo dos referidos serviços.
3.2. Pela prestação dos serviços objeto do presente instrumento, o CONTRATANTE pagará mensalmente a ALGAR TELECOM, os valores constantes na Nota Fiscal Fatura de Prestação de Serviços apresentada pela ALGAR TELECOM ao CONTRATANTE.
3.3. O não pagamento da NFPS na data de seu vencimento sujeitará o CONTRATANTE ao pagamento de multa de 2% (dois por cento) sobre o valor devido, acrescido de atualização pelo IGP-M calculado pela Fundação Getúlio Vargas, bem como, 1% (um por cento) de juros de mora, calculado pro rata die e, ainda:(i) possibilidade de suspensão parcial da prestação do serviço, transcorridos 22 (vinte e dois) dias de vencimento da nota fiscal de prestação de serviço; e (ii) possibilidade de suspensão total da prestação do serviço, transcorridos 30 (trinta) dias do bloqueio parcial, (iii) possibilidade de rescisão contratual, após 30 (trinta) dias do bloqueio total da prestação de serviços.
3.3.1. No caso inadimplência injustificada total ou parcial do CONTRATANTE, a ALGAR TELECOM poderá retirar todos os equipamentos e/ou materiais eventualmente cedidos ao CONTRATANTE, mediante previa notificação.
3.3.2. No caso de inadimplência injustificada total ou parcial do CONTRATANTE, a ALGAR TELECOM poderá no prazo de 15 (quinze) dias contados da data da notificação da existência do débito vencido, reduzir a velocidade dos serviços contratados sem o abatimento proporcional da mensalidade até a regularização do débito e sem o prejuízo da cobrança dos valores contratados, juros e multa.
3.4. As tarifas do(s) SERVIÇO(S) poderão ser reajustadas a cada 12 (doze) meses, de acordo com a variação positiva do IGP-M calculado pela Fundação Getúlio Vargas - FGV ou por qualquer outro índice que venha a substituí-lo. Em caso de majoração das alíquotas tributárias os valores poderão ser repassados ao CONTRATANTE.
3.5. Em caso de utilização dos serviços ora contratados antes da data de ativação total, a ALGAR TELECOM estará autorizada a faturar os SERVIÇOS eventualmente utilizados pelo CONTRATANTE, na forma da regulamentação.
3.6. O não recebimento da fatura ou documento de cobrança mensal até 10 dias da data de seu vencimento implicara na prorrogação da fatura por tantos dias quantos forem os dias de atraso no recebimento do documento de cobrança, sem que incida qualquer ônus ao CONTRATANTE.
3.7. O CONTRATANTE poderá apresentar contestação do seu débito por meio dos telefones 103 12 para a área de concessão da ALGAR TELECOM e 0800 941 2822 para a área de autorização.
3.8 A contestação deverá ser analisada pela ALGAR TELECOM em até 5 (cinco dias) úteis com o envio do parecer ao CONTRATANTE de procedência ou improcedência. Caso haja a necessidade de crédito, este poderá ser feito em conta corrente a ser indicada pelo CONTRATANTE.

CLÁUSULA QUARTA – DOS DIREITOS E OBRIGAÇÕES DO CONTRATANTE

4.1. Sem prejuízo das obrigações assumidas nas demais cláusulas deste instrumento e na legislação aplicável, e responsabilidade do CONTRATANTE:
4.1.1. Utilizar adequadamente o serviço, os equipamentos e as redes de telecomunicações;
4.1.2. Preservar os bens da ALGAR TELECOM e aqueles voltados a utilização do público em geral;
4.1.3. Efetuar o pagamento referente a prestação do serviço, observadas as disposições da legislação aplicável e as obrigações descritas neste Contrato;
4.1.4. Providenciar local adequado e infraestrutura necessários a correta instalação e funcionamento de equipamentos da ALGAR TELECOM, quando for o caso;
4.1.5. Somente conectar à rede da ALGAR TELECOM, terminais que possuam certificação expedida ou aceita pela Anatel.

4.1.6. Mediante prévio aviso, permitir e facilitar o acesso de técnicos da ALGAR TELECOM e prepostos, devidamente credenciados, para eventuais intervenções nos equipamentos instalados em seu ambiente, e que façam parte do objeto deste Contrato, inclusive para manutenção dos equipamentos, devendo ser assegurado o livre desempenho de tais atividades.
4.1.7. Submeter a previa aprovação da ALGAR TELECOM, quaisquer materiais publicitários que envolvam ou mencionem o serviço.
4.1.8. Providenciar equipamento de interconexão de rede dentro dos padrões específicos para o funcionamento do serviço e que obedeça aos requisitos mínimos homologados pela ALGAR TELECOM e ANATEL.
4.1.9. Permitir que a ALGAR TELECOM remova todos os equipamentos, objetos deste e instalados no ambiente do CONTRATANTE, qualquer que seja a forma de cessação ou suspensão do serviço contratado.
4.1.10. Assumir os riscos e responsabilidades inerentes como usuário do serviço, providenciando, se assim entender necessário, sistemas de redundância de telecomunicações, *crash recovery, back-up* de dados permanentes, *no-breaks*, entre outros.
4.1.11. Utilizar os equipamentos colocados à sua disposição exclusivamente para a configuração autorizada, não sendo permitido alterá-los ou ceder a terceiros os equipamentos ou os serviços obtidos por seu intermédio.
4.1.12. Prestar informações necessárias para o melhor cumprimento deste Contrato.
4.1.13 Exigir a observação das normas emanadas pelos órgãos de fiscalização e controle.
4.2. Sem prejuízo das obrigações assumidas nas demais cláusulas deste instrumento e na legislação aplicável, o CONTRATANTE tem direito:
4.2.1. De acesso ao serviço, mediante contratação junto a uma prestadora;
4.2.2. A liberdade de escolha da prestadora;
4.2.3. Ao tratamento não discriminatório quanto as condições de acesso e fruição do serviço;
4.2.4. A informação adequada sobre condições de prestação do serviço, em suas várias aplicações, facilidades adicionais contratadas e respectivos preços;
4.2.5. A inviolabilidade e ao segredo de sua comunicação, respeitadas as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações;
4.2.6. Ao conhecimento prévio de toda e qualquer alteração nas condições de prestação do serviço que lhe atinja direta ou indiretamente;
4.2.7. Ao cancelamento ou interrupção do serviço prestado, a qualquer tempo e sem ônus adicional;
4.2.8. À suspensão do serviço prestado ou à rescisão do contrato de prestação do serviço, a qualquer tempo e sem ônus, ressalvadas as contratações com prazo de permanência
4.2.9. A não suspensão do serviço sem sua solicitação, ressalvada a hipótese de débito diretamente decorrente de sua utilização ou por descumprimento de deveres constantes neste Contrato e da legislação aplicável, notadamente descumprimento do artigo 4o da Lei no 9.472, de 1997;
4.2.10. Ao prévio conhecimento das condições de suspensão do serviço;
4.2.11. Ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela ALGAR TELECOM;
4.2.12. De resposta eficiente e pronta as suas reclamações, pela ALGAR TELECOM;
4.2.13. Ao encaminhamento de reclamações ou representações contra a ALGAR TELECOM, junto a Anatel ou aos organismos de defesa do consumidor (quando aplicável);
4.2.14. A reparação pelos danos causados pela violação dos seus direitos;
4.2.15. A substituição do seu código de acesso, se for o caso, nos termos da regulamentação;
4.2.16. A não ser obrigado ou induzido a adquirir bens ou equipamentos que não sejam de seu interesse, bem como a não ser compelido a se submeter a qualquer condição, salvo diante de questão de ordem técnica, para recebimento do serviço, nos termos da regulamentação;
4.2.17. A ter restabelecida a integridade dos direitos relativos a prestação dos serviços, a partir da purgação da mora, com a imediata exclusão de informação de inadimplência sobre ele anotada, de acordo com o estabelecido neste Contrato;
4.2.18. A ter bloqueado, temporária ou permanentemente, parcial ou totalmente, o acesso a comodidades ou utilidades solicitadas;
4.2.19. A continuidade do serviço pelo prazo contratual, e;
4.2.20. Ao recebimento de documento de cobrança com discriminação dos valores cobrados.

CLÁUSULA QUINTA – DOS DIREITOS E OBRIGAÇÕES DA ALGAR TELECOM

5.1. Sem prejuízo das obrigações assumidas neste instrumento, constituem direitos da ALGAR TELECOM, além dos previstos na Lei no 9.472/97, na regulamentação pertinente e os discriminados no termo de autorização para prestação do SCM:
5.1.1. Empregar equipamentos e infraestrutura que não lhe pertençam;
5.1.2. Contratar com terceiros o desenvolvimento de atividades inerentes, acessórias ou complementares ao serviço, sendo que em qualquer caso a ALGAR TELECOM continuará responsável perante a Anatel e o CONTRATANTE pela prestação e execução do serviço, e;
5.1.3. A ALGAR TELECOM poderá, a seu critério, conceder descontos, realizar promoções, reduções sazonais e reduções em períodos de baixa demanda, entre outras, desde que o faça de forma não discriminatória e segundo critérios objetivos.
5.2. Sem prejuízo das obrigações assumidas nas demais clausulas deste instrumento e na legislação aplicável e responsabilidade da ALGAR TELECOM:
5.2.1. Observar todos os critérios técnicos e operacionais previstos nos documentos que integram este Contrato, conforme aplicável.
5.2.2. Prover a infraestrutura técnica necessária para gerenciar local ou remotamente os serviços adquiridos pelo CONTRATANTE.
5.2.3. Realizar seus melhores esforços para garantir, individualmente, os SLA's eventualmente aplicáveis (Garantia de Desempenho dos Serviços Contratados).
5.2.3.1. Na eventualidade de descumprimento do SLA, serão apurados os eventos de não cumprimento e, constatada a responsabilidade da ALGAR TELECOM, esta deverá realizar os créditos pertinentes ao CONTRATANTE nos futuros documentos de cobrança frente aos serviços contratados. A ALGAR TELECOM não realiza depósitos de numerários ou ressarcimento em espécie.

5.2.3.2. A ALGAR TELECOM utilizara todos os meios comercialmente viáveis para atingir a velocidade ALGAR TELECOM, nos padrões de mercado, quando se tratar de serviços de internet.
5.2.3.3. Em caso de interrupção ou degradação da qualidade do serviço, a prestadora deve descontar da assinatura o valor proporcional ao número de horas ou fração superior a trinta minutos.
5.2.3.4. A necessidade de interrupção ou degradação do serviço por motivo de manutenção, ampliação da rede ou similares deverá ser amplamente comunicada aos assinantes que serão afetados, com antecedência mínima de uma semana, devendo os mesmos terem um desconto na assinatura a razão de 1/30 (um trinta avos) por dia ou fração superior a quatro horas.
5.2.3.5. A ALGAR TELECOM não será obrigada a efetuar o desconto se a interrupção ou degradação do serviço ocorrer por motivos de caso fortuito ou de forca maior, cabendo-lhe o ônus da prova.
5.2.4. É vedado a ALGAR TELECOM condicionar a oferta do serviço a aquisição de qualquer outro serviço ou facilidade, oferecido por seu intermédio ou de suas coligadas, controladas ou controladoras, ou condicionar vantagens ao CONTRATANTE e eventual assinante a compra de outras aplicações ou de serviços adicionais ao ora contratado, ainda que prestados por terceiros.
5.2.5. Não recusar o atendimento a pessoas cujas dependências estejam localizadas na área de prestação do serviço, nem impor condições discriminatórias, salvo nos casos em que a pessoa se encontrar em área geográfica ainda não atendida pela rede, conforme cronograma de implantação constante do termo de autorização para exploração do SCM;
5.2.6. Tornar disponíveis ao CONTRATANTE e assinantes, com antecedência razoável, informações relativas a preços, condições de fruição do serviço, bem como suas alterações;
5.2.7. Descontar do valor da assinatura o equivalente ao número de horas ou fração superior a trinta minutos de serviço interrompido ou degradado em relação ao total médio de horas da capacidade ALGAR TELECOM, conforme aplicável e nos termos e condições descritas neste instrumento;
5.2.8. Tornar disponíveis ao CONTRATANTE, informações sobre características e especificações técnicas dos terminais, necessárias a conexão dos mesmos a sua rede, sendo-lhe vedada a recusa a conectar equipamentos sem justificativa técnica comprovada;
5.2.9. Prestar esclarecimentos ao CONTRATANTE, de pronto e livre de ônus, face a suas reclamações relativas a fruição dos serviços;
5.2.10. Observar os parâmetros de qualidade estabelecidos na regulamentação e neste Contrato, pertinentes a prestação do serviço e a operação da rede;
5.2.11. Observar as leis e normas técnicas relativas a construção e utilização de infraestruturas;
5.2.12. Prestar a Anatel, sempre que solicitado, informações técnico-operacionais ou econômicas, em particular as relativas ao número de assinantes e a área de cobertura e aos valores aferidos pela prestadora em relação aos parâmetros indicadores de qualidade, bem como franquear aos representantes da Anatel o acesso a suas instalações ou a documentação quando solicitado;
5.2.13. Manter atualizados, junto a Anatel, os dados cadastrais de endereço, identificação dos diretores e responsáveis e composição acionaria quando for o caso;
5.2.14. Manter as condições subjetivas, aferidas pela Anatel, durante todo o período de exploração do serviço.
5.2.15. A ALGAR TELECOM observara o dever de zelar estritamente pelo sigilo inerente aos serviços de telecomunicações e pela confidencialidade quanto aos dados e informações do CONTRATANTE, empregando todos os meios e tecnologia necessários para assegurar este direito do CONTRATANTE e respectivos usuários, tornando disponíveis eventuais dados referentes a suspensão de sigilo de telecomunicações para a autoridade judiciária ou legalmente investida desses poderes que determinar a suspensão de sigilo.
5.2.16. A ALGAR TELECOM deverá manter um centro de atendimento ao CONTRATANTE, por meio dos telefones 103 12 para a área de concessão da ALGAR TELECOM e 0800 941 2822 para a área de autorização, com discagem direta gratuita proveniente de terminal fixo ou móvel, durante vinte e quatro horas por dia, sete dias por semana e, atendimento de reclamações e solicitações por meio do *site* *www.algartelecom.com.br*.
5.2.17. O CONTRATANTE poderá ser servido por outras redes ou serviços de telecomunicações, condicionado ao cumprimento das obrigações e condições descritas neste contrato.
5.2.18. A ALGAR TELECOM poderá requerer a restituição de indébito dos tributos incidentes sobre as prestações objeto deste contrato, inclusive em relação àqueles tributos cujo ônus financeiro tenha sido repassado ao CONTATANTE, na forma do art. 166 do Código Tributário Nacional.
5.2.19. Prestar serviços, dentro dos padrões de qualidade e eficiência exigidos para o serviço e nos dispositivos legais e convencionais impostos.
5.2.20. Manter no curso do contrato a sua regularidade fiscal e qualificação técnica exigível para o desempenho do objeto contratual.
5.2.21. Sanar eventuais irregularidades ou correções apontadas pela CONTRATANTE quanto à apresentação de relatórios e/ou de cada etapa dos serviços.
5.2.22. Impedir o acesso à unidade de pessoa que não seja membro de seu corpo técnico com o fim de trabalhar, estagiar ou realizar qualquer atividade similar.

CLÁUSULA SEXTA – DAS OBRIGAÇÕES COMUNS AS PARTES

6.1. O CONTRATANTE reconhece que a ALGAR TELECOM não exerce nenhum controle sobre o conteúdo da informação/dados que transita pela rede do CONTRATANTE. Além disso, e responsabilidade do CONTRATANTE assegurar-se de que a informação/dados que ele e seus usuários transmitem e recebam estão em conformidade com a legislação e regulamentos aplicáveis.
6.2. Nenhuma das Partes deverá, sem consentimento prévio por escrito da outra Parte, divulgar, realizar publicidade ou fazer uso de qualquer informação relativa ao SERVIÇO, a qualquer outra pessoa que não seja alguém por ela contratado para a execução do Contrato. A divulgação a tal pessoa ALGAR TELECOM deverá ser feita somente na medida em que for necessária para fins da citada execução.
6.2.1 As disposições desta cláusula permanecerão válidas e aplicáveis mesmo depois de rescindido ou expirado o Contrato, por qualquer razão que seja, pelo período de 5 (cinco) anos a contar da rescisão ou término do presente Contrato.

CLÁUSULA SÉTIMA – INSTALAÇÃO / MANUTENÇÃO /EQUIPAMENTOS EM COMODATO OU LOCAÇÃO

7.1. A instalação e manutenção dos equipamentos fornecidos pela ALGAR TELECOM a título de comodato ou locação, os quais serão especificados na Nota Fiscal entregue ao CONTRATANTE, ainda que localizados nas dependências do CONTRATANTE, são de competência exclusiva da ALGAR TELECOM, ou seus prepostos, sendo vedada a intervenção de terceiros.

7.2. O CONTRATANTE utilizará os referidos equipamentos colocados à sua disposição pela ALGAR TELECOM exclusivamente para a configuração autorizada, não sendo permitido alterar ou ceder a terceiros os equipamentos ou os SERVIÇOS obtidos por seu intermédio.

7.3. O CONTRATANTE deverá utilizar os equipamentos concedidos em comodato ou locação como se fossem de sua propriedade, não podendo usa-los senão de acordo com a sua própria destinação convencionada pelo contrato, procurando não os desgastar ou desvalorizar, evitando procedimento que possa inferir negligencia ou desídia quanto ao seu uso e gozo.

7.4. O comodato ou locação dos equipamentos vigorara enquanto houver a prestação dos SERVIÇOS, objeto deste, sendo que o CONTRATANTE se obriga a devolvê-los ao final do contrato, em perfeito estado de conservação, ressalvado o desgaste natural decorrente do uso.

7.5. Caberá indenização a ALGAR TELECOM no valor atual de mercado dos bens em questão, se estes vierem a ser furtados, roubados, subtraídos, danificados por culpa ou dolo do CONTRATANTE, ou mesmo caso haja recusa na devolução dos bens.

7.6. O CONTRATANTE se obriga a receber os empregados e prepostos da ALGAR TELECOM, devidamente credenciados, para a manutenção dos equipamentos, devendo ser assegurado o livre desempenho de tais atividades em horário previamente acordado.

7.7. Sendo necessário material de reposição e/ou pecas sobressalentes nos equipamentos disponibilizados pela ALGAR TELECOM, as despesas referentes ao fornecimento e substituição serão de inteira responsabilidade da ALGAR TELECOM. Se a substituição for decorrente de qualquer dano causado por operação indevida pelo CONTRATANTE, as despesas necessárias à recuperação deverão ser integralmente ressarcidas a ALGAR TELECOM.

7.8. Na ocorrência de uma interrupção do SERVIÇO, o CONTRATANTE deverá abrir um chamado de defeito junto ao SAC.

7.9. As alterações na prestação do SERVIÇO, por solicitação do CONTRATANTE, que envolvam mudanças na configuração do referido SERVIÇO, incluindo mudança no local de instalação, serão analisadas pela ALGAR TELECOM quanto a viabilidade técnica e poderão implicar em alterações dos valores a serem pagos pelo CONTRATANTE bem como a possibilidade de rescisão em virtude da inviabilidade.

7.10. Na hipótese de identificação de impossibilidade técnica de instalação dos equipamentos necessários no imóvel do CONTRATANTE para prestação do SERVIÇO ou eventual ausência de autorização do síndico, a ALGAR TELECOM comunicará ao CONTRATANTE tal impossibilidade. Tal impossibilidade, contudo, não caracteriza hipótese de cancelamento do pedido, vez que cabe ao CONTRATANTE, com assessoria da ALGAR TELECOM avaliar as condições técnicas antes da contratação e corrigir os erros encontrados com vistas a garantir a efetividade dos serviços da ALGAR TELECOM.

7.11. Caso o CONTRATANTE solicite visita técnica a ALGAR TELECOM, e se for constatado que não se trata de problema a ser solucionado por esta, poderá ser cobrado do CONTRATANTE o valor de R$ 200,00 (duzentos reais) referente a visita improdutiva.

CLÁUSULA OITAVA – DOS PRAZOS, RENOVAÇÃO E RESCISÃO

8.1. O prazo de vigência do(s) SERVIÇO(S) será o especificado nas Condições Comerciais descritas no Termo de Contratação e a contagem se dará da data da ativação.

8.2. Caso o CONTRATANTE proceda a denúncia, mediante envio de notificação por escrito a ALGAR TELECOM, solicite *downgrade* ou der causa a rescisão e/ou interrupção do SERVIÇO, ficará sujeito ao pagamento de multa compensatória correspondente a um percentual de 30% (trinta por cento) do valor das prestações vincendas, calculada com base no valor da prestação vigente no mês da extinção contratual.

8.2.1. O pagamento da multa estipulada no item acima se dará de uma única vez, depois de transcorridos 30 (trinta) dias da comunicação da denúncia, *downgrade* ou rescisão contratual.

8.2.2. A multa referente a solicitação de *downgrade* corresponderá a um percentual de 30% (trinta por cento) calculada sobre a diferença entre as prestações inicialmente contratadas e as novas prestações ajustadas.

8.2.3. O CONTRATANTE declara ter ciência de que a ALGAR TELECOM realizou determinados investimentos e/ou realizou determinados custos para viabilizar a prestação do serviço objeto deste contrato. Declara ainda que as penalidades previstas neste instrumento são estabelecidas em função de tais investimentos e/ou custos, não podendo, em caso de rescisão e/ou resilição, serem consideradas, para nenhum efeito, como ônus adicional, mas sim integrante da formatação do preço ora praticado.

8.3. Caso qualquer uma das PARTES não tenha interesse na prorrogação do SERVIÇO, deverá comunicar a outra parte por escrito até a data de seu termo. Após o decurso do prazo de vigência inicial descrito neste instrumento, o mesmo poderá ser renovado por meio de aditivo contratual.

8.4. O presente contrato poderá ser rescindido a qualquer tempo com base nos itens abaixo indicados, exclusivamente nos casos em que a parte faltosa, for notificada e não sanar o descumprimento ou não providenciar alternativas de continuidade da prestação com serviços equivalentes ao contratado:

a) Descumprimento ou cumprimento irregular das cláusulas e condições deste contrato, incluindo aquelas referentes a pagamentos;

b) Cancelamento e/ou rescisão, pela ALGAR TELECOM, de serviço considerado imprescindível a prestação do SERVIÇO contratado;

c) Impossibilidade técnica de prestação do SERVIÇO, ainda que superveniente;

d) Transferência de titularidade dos SERVIÇOS pelo CONTRATANTE sem anuência da ALGAR TELECOM;

e) Retirada do SERVIÇO do rol de produtos e serviços oferecidos pela ALGAR TELECOM;

f) Determinação judicial, legal ou regulamentar que impeça a prestação do SERVIÇO;

g) Se quaisquer das Partes ajuizar pedido de recuperação judicial ou ter homologado plano de recuperação extrajudicial, ou lhe for requerida ou decretada falência ou, ainda, quando sua insolvência se manifestar por meio de protestos de títulos de qualquer espécie ou execuções;

h) mediante aviso prévio de 5 (cinco) dias nas seguintes hipóteses:

DS EBDS DS FMSEH DS hugh

h1) de ocorrência de fatos ou situações comprovadamente causadas pela outra Parte e que importem em descrédito comercial da outra Parte;
h2) de caso fortuito ou de forca maior que impeça o cumprimento das obrigações previstas no presente Contrato por prazo superior a 30 (trinta) dias, hipótese em que as Partes ficarão dispensadas de pagar quaisquer indenizações;
h3) em razão da mudança de controle societário de qualquer das Partes ou de sua reorganização societária, através de fusão, incorporação e cisão, salvo se a sociedade sucessora possuir, a critério da outra Parte, capacidade econômica, técnica e financeira para assumir os direitos e obrigações constantes do presente Contrato.
8.5. A critério da ALGAR TELECOM, esta poderá suspender os SERVIÇOS ou rescindi-los caso o CONTRATANTE, seus prepostos ou terceiros a ele vinculados exerçam uma ou mais atividades descritas abaixo:
a) Remeter publicidade de qualquer classe e comunicações com fins de venda ou outras de natureza comercial a uma série de pessoas sem ter sua solicitação prévia ou consentimento (conhecido como *spam)*;
b) Remeter quaisquer outras mensagens não solicitadas nem previamente consentidas a uma serie de pessoas;
c) Enviar cadeias de mensagens eletrônicas não solicitadas nem previamente consentidas;
d) Qualquer atividade que infrinja ou faça uso não apropriado dos direitos de propriedade intelectual de um terceiro, como copyright, marcas registradas, segredos comerciais, pirataria de software, patentes, etc;
e) Promover quaisquer atividades ou ações que violem os direitos de intimidade pessoais de outros, incluindo a coleta e distribuição de informação de usuários da Internet sem sua autorização, exceto quando isto seja permitido pela lei aplicável;
f) Enviar, armazenar, compartilhar, mostrar ou tornar disponível pornografia infantil ou material obsceno;
g) Acessar ilegalmente, sem autorização ou tentar superar medidas de segurança de computadores ou redes que pertençam a um terceiro (conhecido como “hacking”), assim como qualquer atividade previa ao ataque de um sistema para recolher informações sobre ele;
h) Distribuir informação relativa a criação ou transmissão de vírus por Internet, cavalos de Troia, “pinging”, “flooding”, “mailbombing”, “phising” ou ataques de denegação de SERVIÇOS. Também atividades que interrompam ou interfiram no uso efetivo dos recursos da rede de outras pessoas;
i) Usar os SERVIÇOS com propósitos ilegais ou na violação de qualquer lei, regulamento aplicável ou no não cumprimento da política de outros provedores de Internet, sítios web, chats, etc;
j) Quando do uso dos SERVIÇOS, haja indícios de desvio nos padrões técnicos ou fraude;
k) Ajudar ou permitir a qualquer pessoa realizar as atividades descritas anteriormente.

CLAUSULA NONA – DOS PARÂMETROS DE QUALIDADE

9.1. São parâmetros de qualidade para o SCM, sem prejuízo de outros que venham a ser definidos pela Anatel:
9.1.1. Fornecimento de sinais respeitando as características estabelecidas na regulamentação;
9.1.2. Disponibilidade do serviço nos índices contratados;
9.1.3. Emissão de sinais eletromagnéticos nos níveis estabelecidos em regulamentação;
9.1.4. Divulgação de informações aos seus assinantes, de forma inequívoca, ampla e com antecedência razoável, quanto a alterações de preços e condições de fruição do serviço;
9.1.5. Rapidez no atendimento as solicitações e reclamações dos assinantes;
9.1.6. Número de reclamações contra a prestadora;
9.1.7. Fornecimento das informações necessárias a obtenção dos indicadores de qualidade do serviço, de planta, bem como os econômico-financeiros, de forma a possibilitar a avaliação da qualidade na prestação do serviço.

CLÁUSULA DÉCIMA – DA LIMITAÇÃO DE RESPONSABILIDADES

10.1. O presente Contrato é regido pela Lei 10.406/2002 (Código Civil). A responsabilidade relativa a este Contrato será sempre subjetiva e limitar-se-á aos danos diretos/emergentes, desde que devidamente comprovados pela PARTE prejudicada e limitados a média das transações realizadas pelas PARTES no âmbito deste contrato, nos últimos doze meses, imediatamente anteriores ao fato.
10.2. Inobstante outras disposições, em hipótese alguma as PARTES serão responsáveis por danos indiretos ora exemplificados, mas não se limitando a: danos punitivos, especiais, exemplares, incidentais ou por perda de receita e/ou negócios, de dados, de uso de dados, lucros cessantes, uso ou outra vantagem econômica decorrente do contrato ou de qualquer forma a ele relacionada, inclusive, mas não se limitando ao uso ou incapacidade de usar ou prestar os serviços, independentemente da causa, seja em ação contratual, seja por negligencia, limitações ou falhas técnicas impostas as PARTES ou por redes de outras operadoras de serviços de telecomunicações.
10.3. A utilização do serviço é de inteira responsabilidade do CONTRATANTE, não sendo a ALGAR TELECOM responsável por prejuízos que o CONTRATANTE ou terceiros venham a sofrer em virtude de má utilização do serviço, inclusive mas não se limitando a: (i) perda de programas ou de informações; (ii) conteúdo, software, aplicativos, dados armazenados em equipamentos do CONTRATANTE ou da ALGAR TELECOM, bem como por propaganda, produtos, serviços contidos ou oferecidos em sites visitados por meio do acesso fornecido; (iii) danos e prejuízos de qualquer natureza que possam decorrer da presença de vírus ou de outros elementos nocivos nos conteúdos visitados que, de qualquer forma, possam produzir alterações e/ou danos no sistema físico e/ou eletrônico dos equipamentos do CONTRATANTE, ou (iv) pela utilização indevida do serviço por parte do CONTRATANTE.

CLÁUSULA DÉCIMA-PRIMEIRA – DAS CONDIÇÕES GERAIS

11.1. E vedada, sem prévia autorização expressa da ALGAR TELECOM, a cessão ou transferência dos direitos e obrigações tratadas neste Contrato.
11.2. Este documento bem como seus anexos e as modificações previamente e expressamente aceitas pela ALGAR TELECOM, constituem as únicas estipulações reguladoras dos SERVIÇOS.

11.3. O CONTRATANTE declara, sob as penas da lei, que os procuradores e/ou representantes legais que subscrevem este Contrato encontram-se devidamente constituídos na forma dos respectivos Estatutos/Contratos Sociais, com poderes para assumir as obrigações ora contraídas.
11.4. O CONTRATANTE se obriga a devolver, no prazo máximo de 10 (dez) dias a contar do recebimento, todos os contratos, aditivos ou distratos encaminhados para sua assinatura, devidamente assinados, sob pena de suspensão dos SERVIÇOS e aplicação das penalidades descritas no item 8.2, até que o respectivo documento seja devolvido.
11.5. Em qualquer situação regida por este Contrato em que o consentimento, aprovação ou acordo mutuo de qualquer das Partes for necessário, a Parte envolvida concorda em não reter ou retardar, sem justo motivo, tal consentimento ou aprovação.
11.6. O presente Instrumento, juntamente com seus Anexos, constitui títulos executivos extrajudiciais, cobráveis por meio de processo de execução nos termos do Código de Processo Civil.
11.7. Nenhuma tolerância de qualquer uma das Partes no cumprimento pela outra Parte de qualquer dos termos e condições deste Contrato, ou a concessão de prazo por qualquer das Partes a outra Parte irá prejudicar, afetar ou restringir os direitos da respectiva Parte previstos neste Contrato.
11.8. Se qualquer uma das disposições do presente Contrato for ou vier a tornar-se nula ou revelar-se omissa, tal nulidade ou omissão não afetara a validade das demais disposições deste Contrato.
11.9. Na ocorrência de nulidade de clausula contratual que prejudique a eficácia de outras clausulas ou do Contrato em si, as Partes comprometem-se a proceder as alterações necessárias para que o mesmo volte a produzir os efeitos originalmente desejados, dentro de um prazo de 30 (trinta) dias a contar da data de notificação especifica de uma das Partes a outra.
11.10. A Anatel disponibiliza diversos meios para consumidores e a sociedade em geral entrarem em contato para fazer reclamações sobre os serviços das empresas, propor sugestões, tecer críticas e possibilitar acesso ao Regulamento do Serviço de Comunicação Multimídia (“SCM”), mantendo os seguintes canais de atendimento:
11.10.1. Central de Atendimento nº 1331. Pessoas com deficiências auditivas: Ligue 1332 de qualquer telefone adaptado.
11.10.2. Por meio do *site www.anatel.gov.br.*
11.10.3. Por meio de correspondência para o endereço: Assessoria de Relações com o Usuário – ARU (Endereço: SAUS, Quadra 06, Bloco F, 2o andar, Brasília - DF, CEP: 70.070-940).
11.10.4. Para dar completa aplicabilidade à cláusula 5.2.18, o CONTRATANTE autoriza expressamente a ALGAR TELECOM a requerer a restituição dos tributos indevidamente pagos sobre o(s) SERVIÇO(S) retratado(s) neste contrato, especialmente em relação aos tributos cujo ônus financeiro tiver sido a ele repassado.
11.11. O presente contrato não gera vinculo de natureza trabalhista e/ou previdenciária entre as partes, respondendo cada uma delas pelas obrigações relativas à mão de obra que utilizar para a execução deste Contrato.
11.12. O CONTRATANTE declara e aceita que as condições comerciais previstas no Termo de Contratação poderão, se descritas expressamente no respectivo documento, ser consideradas tendo em vista o conjunto do projeto elaborado para atendimento do CONTRATANTE (“Pacote”). Deste modo, se houver cancelamento ou *downgrade* de um ou mais serviços que compõem o “Pacote” descrito no Termo de Contratação, fica estabelecido que a ALGAR TELECOM poderá rever as condições comerciais/valores ofertados para cada um dos serviços isoladamente com o objetivo de garantir o equilíbrio econômico do contrato, podendo inclusive faturar cada um dos serviços de acordo com preços e condições ofertadas para estes individualmente conforme condições comerciais vigentes à época do cancelamento ou descritas no termo.

CLÁUSULA DÉCIMA-SEGUNDA – DAS DECLARAÇÕES E GARANTIAS ANTICORRUPÇÃO

12.1. As PARTES declaram e garantem que não admitem nem toleram condutas que possam caracterizar corrupção seja ela passiva ou ativa, seja por si e/ou por seus representantes, devendo envidar todos os esforços necessários, cuidado e diligência os quais deveria empregar nas atividades dos seus próprios negócios para que haja sempre o respeito às normas, políticas e legislações pertinentes. Ocorrendo fato dessa natureza, o presente contrato poderá ser rescindido imediatamente.
12.2. No desempenho das obrigações previstas no Contrato, as PARTES comprometem-se, por si, seus empregados, subcontratados e pessoas físicas ou jurídicas a eles relacionadas, a não pagar ou oferecer qualquer coisa de valor relevante, seja como compensação, presente ou contribuição ou valor em espécie, a qualquer pessoa ou organização, privada ou governamental, se tais pagamentos, contribuições e presentes forem ou puderem ser considerados ilegais ou duvidoso.
12.3. A CONTRATADA por si e por seus sócios, administradores, gestores, representantes legais, empregados, prepostos e subcontratados (“Colaboradores”), se compromete a adotar os mais altos padrões éticos de conduta na condução dos seus negócios e não pagar, prometer ou autorizar o pagamento de qualquer valor ou oferecer qualquer tipo de vantagem indevida direta ou indiretamente, a qualquer Funcionário Público ou a terceira pessoa, bem como garante que não emprega e não empregará, direta ou mediante contrato de serviços ou qualquer outro instrumento, trabalho escravo, trabalho infantil.
12.4. A CONTRATADA declara, sob as penas da lei, que não esteve envolvida com qualquer alegação de crime de lavagem de dinheiro, delito financeiro, financiamento de atividades ilícitas ou atos contra a Administração Pública, incluindo, mas não se limitando a corrupção, fraude em licitações, suborno ou corrupção e que durante a
prestação dos serviços ora avençado, cumprirá com todas as leis aplicáveis à natureza dos serviços contratados, em especial a Lei de Improbidade Administrativa e Lei Brasileira Anticorrupção.

CLÁUSULA DÉCIMA TERCEIRA – DO ENDEREÇO PARA FINS DE CITAÇÃO/INTIMAÇÃO EM EVENTUAL LITIGIO JUDICIAL E DO FORO

13.1. Para fins de eventual demanda judicial, as PARTES consideram que a citação de ambas poderá ser feita exclusivamente sob a inteligência do §1º do art. 269 do CPC/15, em endereços físicos ou eletrônicos descritos em campo específico no Termo de Contratação e/ou neste instrumento, mediante o envio de uma parte a outra de comunicação expressa referente ao processo judicial, sendo que as partes declaram e concordam que o envio de e-mail para o endereço informado pelas partes convalidará a respectiva citação, conforme permitido pelo art. 190 do mesmo diploma legal.

13.1.1. As PARTES se comprometem em informar sobre qualquer alteração do endereço físico/eletrônico, sob pena de considerar válida a citação positiva promovida perante o ato.
13.1.2. As PARTES estipulam o prazo de 10 (dez) dias corridos contados do envio para que a citação via meio físico ou eletrônico sejam lidas. Após esse período, a citação será considerada ficta ou seja, realizada nos temos da Legislação vigente. Os prazos processuais terão início no primeiro dia útil após o dia do registro da ciência.
13.1.3. As partes declaram que tem conhecimento e aceitam que foram oferecidos para o CONTRATANTE canais de atendimento conforme determinação da ANATEL e que o endereço indicado no Termo de Contratação, no campo "e-mail para fins judiciais" se destina exclusivamente para o recebimento de citações, intimações, atos judiciais ou atividades dele decorrentes. Toda e qualquer mensagem não relacionada a processos judiciais não será recebida e/ou analisada sendo considerada como não recebida.
13.1.4. Independentemente do foro, os únicos endereços físico e eletrônico para onde podem ser enviadas as correspondências a que se refere esta cláusula, sob pena de nulidade e/ou não recebimento são:

ENDEREÇO FISICO DA ALGAR:

ALGAR MULTIMIDIA S/A: Rua Jose Alves Garcia, nº 415, Mezanino, bairro Brasil, na cidade de Uberlândia, Estado de Minas Gerais.
ALGAR TELECOM S/A: Rua Jose Alves Garcia, nº 415, bairro Brasil, na cidade de Uberlândia, Estado de Minas Gerais.
ALGAR SOLUÇÕES EM TIC S/A: Rua José Alves Garcia, nº 415, Bloco A, bairro Brasil, na cidade de Uberlândia, Estado de Minas Gerais.

ENDEREÇO ELETRÔNICO – E-MAIL: citacao@algartelecom.com.br

13.2. Fica acordado entre as partes que qualquer documentação administrativa ou judicial somente terá validade se direcionada à CONTRATANTE, para o seguinte endereço: Rua Av. Areião, Qd. 17, Lt. 23, CEP: 74820-370, Setor Pedro Ludovico, Goiânia – Goiás.
13.3. As PARTES elegem o foro da comarca de Goiânia/GO, para dirimir quaisquer questões decorrentes deste contrato, com expressa renuncia a qualquer outro, por mais privilegiado que seja.

DADOS DO CONTRATANTE

Nome / Razão Social: **INSTITUTO BRASILEIRO DE GESTÃO HOSPITALAR IBGH**			
CPF / CNPJ: **18.972.378/0009-70**		I.E.: "	
Endereço : **Av. V-5, S/N, Qd. A, Área Lt.001-E SALA 01**			
Bairro: **Cidade Vera Cruz**	CEP: **74936-600**	Cidade: **Aparecida de Goiânia**	UF: **GO**

CONTATO TÉCNICO

Nome	**Jefferson Tadeu**
Telefone	**(62) 98406-1362**

DADOS CONTRATUAIS

Prazo Contratual	**12 meses**
Fator de Correção	**IGP-M**

DADOS DO PRODUTO

Nº Serviço	Produto / Componente	Prazo de Execução (Dias úteis)	Custo de Instalação	Custo Mensal (Sem Impostos)	Custo Mensal (Com Impostos)
A definir	**Internet Link**	**30 dias**	**Isento**	**R$ 1.587,80**	**R$ 2.135,00**
Atributo			**Valor**		
Quantidade de Endereços IP			**8 (5 disponíveis)**		
Tipo			**IPV4**		
Velocidade			**200 Mbps**		
Nº Serviço	Produto / Componente	Prazo de Execução (Dias úteis)	Custo de Instalação	Custo Mensal (Sem Impostos)	Custo Mensal (Com Impostos)
A definir	**Gerenciamento de rede - NOC**	**30 dias**	**Isento**	**R$ 78,99**	**R$ 89,00**
Nº Serviço	Produto / Componente	Prazo de Execução (Dias úteis)	Custo de Instalação	Custo Mensal (Sem Impostos)	Custo Mensal (Com Impostos)
A definir	**Anti-DDoS**	**30 dias**	**Isento**	**R$ 732,19**	**R$ 825,00**
Nº Serviço	Produto / Componente	Prazo de Execução (Dias úteis)	Custo de Instalação	Custo Mensal (Sem Impostos)	Custo Mensal (Com Impostos)
A definir	**SOC AVANÇADO FG200-E**	**30 DIAS**	**ISENTO**	**R$ 2.099,92**	**R$ 2.350,00**

DADOS DE INSTALAÇÃO

Endereço: **Av. V-5, S/N, Qd. A, Área Lt.001-E SALA 01**			
Bairro: **Cidade Vera Cruz**	CEP: **74936-600**	Cidade: **Aparecida de Goiânia**	UF: **GO**

DADOS DE FATURAMENTO

Nome / Razão Social: **INSTITUTO BRASILEIRO DE GESTÃO HOSPITALAR IBGH**			
CPF/CNPJ: **18.972.378/0009-70**			
Endereço: **Av. V-5, S/N, Qd. A, Área Lt.001-E SALA 01**			
Bairro: **Cidade Vera Cruz**	CEP: **74936-600**	Cidade: **Aparecida de Goiânia**	UF: **GO**

TOTAIS

CONDIÇÃO ESPECIAL - PROJETO - "PACOTE" * (**X**) SIM NÃO ( )
CONDIÇÕES COMERCIAIS VINCULADAS AO CONTRATO: INTERNET LINK, NOC, ANTI-DDoS, FIREWALL E SD-WAN.

Total do custo mensal recorrente	**R$ 5.399,00**
Total do custo não recorrente	**R$ 0,00**

Goiânia, 11 de fevereiro de 2020.

Assinatura **CONTRATANTE:** DocuSigned by: Elinde Bento da Silva B6DEAC069BCD401...
Nome:
Cargo:

Assinatura **ALGAR TELECOM**: DocuSigned by: Federico Miguel Silva E Henriques 5093F2ED6C0A48E...
Nome:
Cargo:

DocuSigned by: Hugo Correia da Silva 179E982B515246C...
Nome:
Cargo:

TESTEMUNHAS:

Nome:
CPF: DocuSigned by: Ana Paula Freitas A43FE7416A744AA...

Nome:
CPF: DocuSigned by: Carlos Costa Pinto Neto D4F71B85D6CE4C4...

ANEXO I – FILIAIS

FILIAIS - ALGAR MULTIMIDIA S/A								
CNPJ	**Inscrição Estadual**	**Cidade**	**UF**	**Logradouro**	**N°**	**Complemento**	**Bairro**	**CEP**
04.622.116/0001-13	001.030.140.00-75	UBERLANDIA	MG	R JOSE ALVES GARCIA	415	MEZANINO	BRASIL	38.400-668
04.622.116/0010-04	10.420617-9	ITUMBIARA	GO	R PADRE FELIX	1	Térreo – Sala 02	CENTRO	75.503-130
04.622.116/0011-95	149.666.183.110	SAO PAULO	SP	R. QUATA	807	ANDAR 1	VILA OLIMPIA	04.546-044
04.622.116/0012-76	07.494.911/002-02	BRASILIA	DF	ST SHIS QI 11 BLOCO K SALAS 102 E	103	PAVIMENTO SUPERIOR	LAGO SUL	71.625-590
04.622.116/0016-08	78.562.749	RIO DE JANEIRO	RJ	AV RIO BRANCO	1	SALA: 1503 – PARTE	CENTRO	20.090-003
04.622.116/0017-80	90454146-01	CURITIBA	PR	R PASTEUR	463	Conj 201 Edif Centro Empr. Jatobá	BATEL	80.250-080
04.622.116/0020-86	28.353.369-2	PARANAIBA	MS	R GENEROSO PONCE	1609		CENTRO	79.500-000
04.622.116/0023-29	096/3414194	PORTO ALEGRE	RS	AV PROTASIO ALVES	3405	PARTE 2 CONJ 101	PETROPOLIS	90.410-003
04.622.116/0024-00	25.666.501-0	FLORIANOPOLIS	SC	AV AFONSO PENA	**384**	ANDAR 1 SALA 2	ESTREITO	88.070-650
04.622.116/0027-52	15.303.599-4	BELEM	PA	R MUNICIPALIDADE	1646	SALA B	UMARIZAL	66.050-350
04.622.116/0028-33	082.728.30-5	VITORIA	ES	R GENERAL OSORIO	83	SALA 108	CENTRO	29.010-911
04.622.116/0029-14	88657457	SALVADOR	BA	EST CAMPINAS PIRAJA	27	Sala: 108 Parte B	CAMPINAS DE PIRAJA	41.270-000

FILIAIS – ALGAR TELECOM S/A								
Cidade	**UF**	**CNPJ**	**INSC_ESTADUAL**	**Logradouro**	**N°**	**Complemento**	**Bairro**	**CEP**
UBERLANDIA	MG	71.208.516/0001-74	702.98094500-10	R JOSE ALVES GARCIA	415		BRASIL	38.400-668
ITUMBIARA	GO	71.208.516/0103-07	101.530.595	R PADRE FELIX	01		SETOR CENTRAL	75.503-130
PARANAIBA	MS	71.208.516/0109-94	28.257604-5	R GENEROSO PONCE	1609		CENTRO	79.500-000
FRANCA	SP	71.208.516/0119-66	310.075.186.111	R MONSENHOR ROSA	1989		CENTRO	14.400-670
FLORIANOPOLIS	SC	71.208.516/0161-78	254949398	R AFONSO PENA	384	1 ANDAR, SL 1 - PARTE	ESTREITO	88.070-650
PORTO ALEGRE	RS	71.208.516/0162-59	096/3056980	AV PROTASIO ALVES	3405	PARTE CJ-101	PETROPOLIS	90.410-003
BOA VISTA	RR	71.208.516/0163-30	240118316	R JOCA FARIAS	932	-PARTE	CARANA	69.313-612
SALVADOR	BA	71.208.516/0164-10	65155796	R ESTRADA DE CAMPINAS	27	S/108 PARTE	CAMPINAS DE PIRAJA	41.275-270
OLINDA	PE	71.208.516/0165-00	18.1.660.0311152-8	R CORDOBA	69	APTO 01 - PARTE	JD ATLANTICO	53.140-071
MACAPA	AP	71.208.516/0166-82	03027877-5	AV MAMEDE A. DA SILVA	138	PARTE	JD. EQUATORIAL	68.901-092
BELEM	PA	71.208.516/0167-63	15.240.122-9	R MUNICIPALIDADE	1754	SALA B PARTE	UMARIZAL	66.050-350
SAO CRISTOVAO	SE	71.208.516/0168-44	27.109.526-1	R D COUNTRY CLUB	81	PARTE	COUNTRY CLUB	49.100-000
JOAO PESSOA	PB	71.208.516/0169-25	16.142.421-0	R INDIO PIRAGIBE	327	SALA 205 - PARTE	VARADOURO	58.011-200
CUIABA	MT	71.208.516/0170-69	13281112-0	R GENERAL VALLE	321	SALA 1502	BANDEIRANTES	78.010-000
RIO DE JANEIRO	RJ	71.208.516/0171-40	77700501	AV RIO BRANCO	01	SALA 1504	CENTRO	20.090-907
VITORIA	ES	71.208.516/0172-20	082.265.03-8	R GENERAL OSORIO	83	SALA 109 - PARTE	CENTRO	29.010-911
BRASILIA	DF	71.208.516/0173-01	07.462.384/002-66	OTR SHIS QI 11 BLOCO K, SALA 101	S/N	PAVIMENTO SUPERIOR	LAGO SUL	71.625-205
TERESINA	PI	71.208.516/0174-92	19454382-0	R SAO PEDRO	1695	APTO.02-PARTE	CENTRO	64.001-260
RIO BRANCO	AC	71.208.516/0175-73	01.015.653/001-26	R MARECHAL DEODORO	871	SALA 09	CENTRO	69.900-210
MACEIO	AL	71.208.516/0176-54	24104364-6	R DA ALEGRIA	36	SALA 12 - 1 ANDAR	CENTRO	57.020-320
MANAUS	AM	71.208.516/0177-35	04212438-7	TV SERGIO MILIETE	10	QUADRA: 14; CONJ: VILA NOVA; ANTIGA RUA 8	CIDADE NOVA	69.099-124
CURITIBA	PR	71.208.516/0178-16	90322164-01	R PASTEUR	463	CONJ 201 EDIF CENTRO EMPR JATOBA	BATEL	80.250-080
NATAL	RN	71.208.516/0179-05	20098165-0	R MARECHAL FLORIANO PEIXOTO	259	A PARTE	PETROPOLIS	59.020-500
PORTO VELHO	RO	71.208.516/0180-30	1282948	R SALVADOR DALI	7398		CUNIA	78.909-525
PALMAS	TO	71.208.516/0181-11	29383717-1	Q 206 SUL ALAMEDA15, LOTE 01	S/N	APTO 01 SALA 03	PLANO DIRETOR SUL	77.020-518
FORTALEZA	CE	71.208.516/0182-00	06.692760-9	R JOSE GOMES DE MOURA	91	SALA 312 - PARTE	CENTRO	60.040-010
SAO LUIS	MA	71.208.516/0183-83	12.215.271-9	R ALCANTARA	16	QUADRA 13	PARQUE PINDORAMA	65.041-191
FILIAIS - ALGAR SOLUÇÕES EM TIC S/A								

201917249158-1

CNPJ	Nome Empresa	Inscrição Estadual	Endereço	Nº	Complemento	CEP	Bairro	Cidade	UF
22.166.193/0001-98	ALGAR SOLUCOES EM TIC S/A	0027119860089	R JOSE ALVES GARCIA	415	BLOCO A	38.400-668	BRASIL	UBERLANDIA	MG
22.166.193/0010-89	ALGAR SOLUCOES EM TIC S/A	106724622	R PADRE FELIX	1	TERREOPARTE	75.503-130	SETOR CENTRAL	ITUMBIARA	GO
22.166.193/0011-60	ALGAR SOLUCOES EM TIC S/A	87280454	AV RIO BRANCO	1	SALA 1503 PARTE 3	20.090-003	CENTRO	RIO DE JANEIRO	RJ
22.166.193/0012-40	ALGAR SOLUCOES EM TIC S/A	90734243-37	R PASTEUR	463	ANDAR 2 SALA 201 EDIFICIO CENTRO EMPRESARIAL JATOBA	80.250-080	BATEL	CURITIBA	PR
22.166.193/0013-21	ALGAR SOLUCOES EM TIC S/A	258129379	R 1536	60	SALA 503	88.330-610	CENTRO	BALNEARIO CAMBORIU	SC
22.166.193/0014-02	ALGAR SOLUCOES EM TIC S/A	054/0041653	R PEDRO TONIOLO	1170	PARTE	99.900-000	INDUSTRIAL	GETULIO VARGAS	RS
22.166.193/0015-93	ALGAR SOLUCOES EM TIC S/A	002711986.01-60	AV JOSE ANDRAUS GASSANI	4555	PARTE	38.402-324	DISTRITO INDUSTRIAL	UBERLANDIA	MG
22.166.193/0016-74	ALGAR SOLUCOES EM TIC S/A	07.787.099/002-96	ST SCN QUADRA 1 BLOCO C	S/N	SALA 1913	70.711-902	ASA NORTE	BRASILIA	DF
22.166.193/0017-55	ALGAR SOLUCOES EM TIC S/A	Processo de centralização	R NICOLAU BARRETO	S/N	0	88.336-335	NOVA ESPERANCA	BALNEARIO CAMBORIU	SC
22.166.193/0018-36	ALGAR SOLUCOES EM TIC S/A	141492984115	R QUATA	807	ANDAR 1 PARTE	04.546-044	VILA OLIMPIA	SAO PAULO	SP
22.166.193/0019-17	ALGAR SOLUCOES EM TIC S/A	258421118	R EMILIO BLUM	131	SALA 705 PAVMTO7	88.020-010	CENTRO	FLORIANOPOLIS	SC
22.166.193/0020-50	ALGAR SOLUCOES EM TIC S/A	0765629-72	R PADRE CARAPUCEIRO	706	SALA 1702 EDF CTR EMP TORRE CARLOS PENA FILHO	51.020-280	BOA VIAGEM	RECIFE	PE
22.166.193/0021-31	ALGAR SOLUCOES EM TIC S/A	06.760444-7	AV SANTOS DUMONT	1510	SALA 101 A 109	60.150-161	ALDEOTA	FORTALEZA	CE
22.166.193/0022-12	ALGAR SOLUCOES EM TIC S/A	163186251	R ABELARDO DA SILVA GUIMARAES BARRETO	51	SALA 1201 E 1202 BLOCO C	58.046-110	ALTIPLANO CABO BRANCO	JOAO PESSOA	PB
22.166.193/0023-01	ALGAR SOLUCOES EM TIC S/A	06.760444-7	R SATIRO DIAS	308	0	60.420-430	MONTESE	FORTALEZA	CE
22.166.193/0024-84	ALGAR SOLUCOES EM TIC S/A	271599480	AV DOUTOR JOSE MACHADO DE SOUZA	220	SALA 706	49.025-740	JARDINS	ARACAJU	SE
22.166.193/0025-65	ALGAR SOLUCOES EM TIC S/A	247.62525-6	R JOSE SOARES SOBRINHO	119	SALA 509 - A	57.036-640	JATIUCA	MACEIO	AL
22.166.193/0026-46	ALGAR SOLUCOES EM TIC S/A	204961904	R DOS CAICOS	1259	0	59.037-700	ALECRIM	NATAL	RN
22.166.193/0027-27	ALGAR SOLUCOES EM TIC S/A	083.484.47-7	AV NOSSA SENHORA DOS NAVEGANTES	955	SALA 1703	29.050-335	ENSEADA DO SUA	VITORIA	ES
22.166.193/0028-08	ALGAR SOLUCOES EM TIC S/A	163186251	AV DOM PEDRO II	1715	0	58.040-440	TORRE	JOAO PESSOA	PB
22.166.193/0029-99	ALGAR SOLUCOES EM TIC S/A	083.484.47-7	AV 5ª AVENIDA	37	0	29.111-175	COBILANDIA	VILA VELHA	ES
22.166.193/0030-22	ALGAR SOLUCOES EM TIC S/A	204961904	R DOUTOR POTY NOBREGA	1946	SALA 1005 E 1006	59.056-180	LAGOA NOVA	NATAL	RN
22.166.193/0031-03	ALGAR SOLUCOES EM TIC S/A	247.62525-6	R DOM SANTINO COUTINHO	46	GALPAOA	57.052-070	PITANGUINHA	MACEIO	AL
22.166.193/0032-94	ALGAR SOLUCOES EM TIC S/A	Centralizada	R SOLDADO LUIZ GONZAGA DAS VIRGENS	111	SALA 402	41.820-560	CAMINHO DAS ARVORES	SALVADOR	BA
22.166.193/0033-75	ALGAR SOLUCOES EM TIC S/A	096/3744240	R MANOELITO DE ORNELLAS	55	SALA 601 5 ANDAR TORRE A	90.110-230	PRAIA DE BELAS	PORTO ALEGRE	RS
22.166.193/0034-56	ALGAR SOLUCOES EM TIC S/A	271599480	R RIO GRANDE DO SUL	620	GALPÃO632	49.075-510	SIQUEIRA CAMPOS	ARACAJU	SE
22.166.193/0035-37	ALGAR SOLUCOES EM TIC S/A	153162426	R DOUTOR ALTINO TEIXEIRA	1579	GL	41.233-010	PORTO SECO PIRAJA	SALVADOR	BA
22.166.193/0036-18	ALGAR SOLUCOES EM TIC S/A	Centralizado	R CASA DO ATOR	415		04546-001	VILA OLIMPIA	SÃO PAULO	SP
22.166.193/0037-07	ALGAR SOLUCOES EM TIC S/A	Centralizada	AV GETULIO VARGAS	299	0	38700128	CENTRO	PATOS DE MINAS	MG
22.166.193/0038-80	ALGAR SOLUCOES EM TIC S/A	Centralizada	R GOVERNADOR VALADARES	61	PARTE	38.010-380	CENTRO	UBERABA	MG
22.166.193/0039-60	ALGAR SOLUCOES EM TIC S/A	Centralizada	AV DOM JOAO VI	49	SALA 01E02	30570063	CINQUENTENARIO	BELO HORIZONTE	MG
22.166.193/0040-02	ALGAR SOLUCOES EM TIC S/A	Centralizada	R VINTE E QUATRO	945	PARTE II	38.300-078	CENTRO	ITUITABA	MG
22.166.193/0041-85	ALGAR SOLUCOES EM TIC S/A	Centralizada	R BENEDITO VALADARES	162	0	35.600-630	CENTRO	PARÁ DE MINAS	MG
22.166.193/0042-66	ALGAR SOLUCOES EM TIC S/A	Centralizada	R RIO GRANDE DO NORTE	3260	BLOCO 3	38.405-321	BRASL	UBERLANDIA	MG
22.166.193/0043-47	ALGAR SOLUCOES EM TIC S/A	Centralizada	AV JOSE ANDRAUS GASSANI	4901	BL C SALA 05	38.402-324	DISTRITO INDUSTRIAL	UBERLANDIA	MG
22.166.193/0044-28	ALGAR SOLUCOES EM TIC S/A	Centralizada	RUA CORONEL JOSÉ DE PAULA	300	PARTE C	38.200-000	CENTRO	FRUTAL	MG
22.166.193/0045-09	ALGAR SOLUCOES EM TIC S/A	Centralizada	AV OLIMPIO JACINTO DA SILVA	1280	PARTE C	38.071-660	JARDIM ELDORADO	UBERABA	MG
22.166.193/0046-90	ALGAR SOLUCOES EM TIC S/A	Centralizada	R ANHANGA QUADRA 178, LOTE 08	682	BLOCO B	74.835-130	PARQUE AMAZONIA	GOIANIA	GO

22.166.193/0047-70	ALGAR SOLUCOES EM TIC S/A	Centralizada	R SILVIO BIVAR SCHMITT	545		95.045.135	CENTENARIO	CAXIAS DO SUL	RS
22.166.193/0048-51	ALGAR SOLUCOES EM TIC S/A	Centralizada	AV JAIME LACERDA	220	SALA 02	38.280-000	VILA PADUA	ITURAMA	MG
22.166.193/0049-32	ALGAR SOLUCOES EM TIC S/A	Centralizado	PC SETE DE SETEMBRO	397	SALA 02	14.600-000	CENTRO	SAO JOAQUIM DA BARRA	SP
22.166.193/0050-76	ALGAR SOLUCOES EM TIC S/A	Centralizado	R FLORIANO PEIXOTO	998	SALA 02	14.400-760	CENTRO	FRANCA	SP
22.166.193/0051-57	ALGAR SOLUCOES EM TIC S/A	Centralizado	R MONSENHOR ROSA	1989		14.400-670	CENTRO	FRANCA	SP
22.166.193/0052-38	ALGAR SOLUCOES EM TIC S/A	Centralizado	AV ROMEU STRAZZI	325	SALA 409 ANDAR 4	15.084-010	VILA SINIBALDI	SAO JOSE DO RIO PRETO	SP
22.166.193/0054-08	ALGAR SOLUCOES EM TIC S/A	Centralizado	R MANOELITO DE ORNELLAS	55	SALA 601 ANDAR 5 TORRE A	90.110-230	PRAIA DE BELAS	PORTO ALEGRE	RS
22.166.193/0055-80	ALGAR SOLUCOES EM TIC S/A	Centralizado	AV COMANDANTE SALGADO	893	SALA 02	14.300-220	CASTELO	BATATAIS	SP
22.166.193/0056-61	ALGAR SOLUCOES EM TIC S/A	Centralizado	AV DOUTOR ANGELO SIMOES	694		13.041-150	JARDIM LEONOR	CAMPINAS	SP
22.166.193/0057-42	ALGAR SOLUCOES EM TIC S/A	Centralizado	R AMADOR BUENO	1400		14.010-070	CENTRO	RIBEIRAO PRETO	SP
22.166.193/0058-23	ALGAR SOLUCOES EM TIC S/A	Centralizado	AV BARAO DE ITAPURA	2294	EDIF MONTPELLIER ANDAR 11 SALA 115 A 119	13.073-300	JARDIM GUANABARA	CAMPINAS	SP
22.166.193/0059-04	ALGAR SOLUCOES EM TIC S/A	Centralizado	R VINTE E OITO DE SETEMBRO	2075		13.560-270	CENTRO	SAO CARLOS	SP
22.166.193/0060-48	ALGAR SOLUCOES EM TIC S/A	Centralizado	R BARAO DE TEFFE	1000	SALA 34	13.208-761	JARDIM ANA MARIA	JUNDIAI	SP
22.166.193/0061-29	ALGAR SOLUCOES EM TIC S/A	Centralizado	R SINVAL CORREA	104	GALPAO 103	36.020-310	VILA OZANAN	JUIZ DE FORA	MG
22.166.193/0062-00	ALGAR SOLUCOES EM TIC S/A	Em processo	R JOAO DE ABREU	192	QD F8 LT 24 EDIF ATON BUSINESS STYLE ANDAR 11 L B111 A B114	74.120-110	SETOR OESTE	GOIANIA	GO
22.166.193/0063-90	ALGAR SOLUCOES EM TIC S/A	15.650.856-7	R DA PAZ I	1-A	QUADRA07 SALA 201	66.640-620	MANGUEIRAO	BELEM	PA
22.166.193/0064-71	ALGAR SOLUCOES EM TIC S/A	0778709900105	RUA 3 CHACARA 47	5B	TERREO	72.005-680	SETOR HABITACIONAL VICENTE PIRES	BRASILIA	DF

DS EBDS DS FMSEH DS hugh

ANEXO II - ACORDO DE NÍVEIS DE SERVIÇOS - *Service Level Agreement* - SLA

1. OBJETIVO

1.1. O presente Acordo tem por objetivo o comprometimento mútuo em relação às obrigações definidas neste Contrato, PROPOSTA COMERCIAL e/ou TERMO DE CONTRATAÇÃO, exclusivamente para prestação dos serviços de comunicação multimídia da ALGAR TELECOM.

1.2. A ALGAR TELECOM alocará recursos e sistemas de suporte de forma a garantir ao CONTRATANTE as melhores condições de acesso e transporte das informações e de utilização dos recursos pertinentes aos serviços oferecidos, respeitando-se o escopo definido para os mesmos.

1.3. Constituem ainda objetivo deste Acordo:

1.3.1. Pesquisa e entendimento das necessidades do CONTRATANTE;

1.3.2. Garantia de que os objetivos do CONTRATANTE estão alinhados com os objetivos da ALGAR TELECOM;

1.3.3. Estabelecimento claro de metas e objetivos a serem atingidos; e,

1.3.4. Definição clara de responsabilidades.

2. DESCRIÇÃO DOS SERVIÇOS CONTRATADOS

2.1. As descrições e especificações dos serviços contratados são as constantes do Contrato, PROPOSTA COMERCIAL e/ou TERMO DE CONTRATAÇÃO os quais fazem parte integrante e indissociável do presente instrumento.

3. DEFINIÇÃO DE ACORDO DE NÍVEIS DE SERVIÇOS

3.1. Denomina-se acordo de nível de serviço ou SLA (*Service Level Agreement*), para efeito do presente contrato, o nível de desempenho técnico do serviço prestado proposto pela ALGAR TELECOM, sendo certo que tal acordo não representa diminuição de responsabilidade da ALGAR TELECOM, mas sim indicador de excelência técnica.

4. NÍVEIS DE SERVIÇOS ACORDADOS

4.1. A ALGAR TELECOM, desde que observadas as obrigações a cargo do CONTRATANTE e previstas no presente Acordo e demais documentos integrantes do presente instrumento, tem condição técnica de oferecer e se propõe a manter um SLA (*Service Level Agreement* – acordo de nível de serviços ou garantia de desempenho) de manutenção da disponibilidade dos serviços envolvidos na solução objeto do SERVIÇO, em 99,5% (noventa e nove vírgulas cinco por cento) do tempo, em cada mês civil.

4.2. O percentual de indisponibilidade deverá ser calculado de acordo com a seguinte fórmula:

Indisponibilidade = (TR/43200) * 100, onde TR = Σ “Tempo de Reparo por Interrupção” ocorridos no mês, em minutos.

4.3. Deverá ser considerado como indisponível, somente o tempo de interrupções não previstas, reservando para posterior negociação os períodos de manutenção preventiva ou corretiva a serem planejados com antecedência de, no mínimo, uma semana.

5. TIPOS DE OCORRÊNCIA

5.1. Para efeito de contagem das métricas de disponibilidade e tempo de reparo dos serviços, deverão ser considerados os seguintes tipos de ocorrência:

5.1.1 Interrupção: quando o CONTRATANTE se encontra impossibilitado do uso dos recursos em função de indisponibilidade causada por culpa comprovadamente atribuível exclusivamente à ALGAR TELECOM.

6. TEMPO DE ATENDIMENTO E RESPOSTA

6.1. Para efeito de contagem da métrica de tempo de atendimento, deverão ser considerados os seguintes tipos de ocorrência, os quais não são considerados no cálculo das métricas de disponibilidade e tempo de reparo do serviço:

6.1.1. Requisição: quando o CONTRATANTE solicita algum serviço adicional ou novo serviço.

6.1.2. Ajuda: quando o CONTRATANTE solicita ajuda para utilização e/ou operação dos recursos relacionados aos serviços providos pela ALGAR TELECOM.

6.2. O tempo de atendimento é o tempo corrente desde a abertura de chamado pelo CONTRATANTE até o seu completo atendimento, seja quando da ativação do novo serviço, para os eventos do tipo “Requisição”, ou quando do provimento da informação solicitada, para os eventos do tipo “Ajuda”.

6.3. O tempo de atendimento não deverá ser superior a 72 (setenta e duas) horas, salvo nos casos onde o atendimento à solicitação gerar interrupção do serviço. Nestes casos, o tempo de atendimento deve atender o planejamento de implementação deste novo serviço, a ser acordado entre as partes.

6.4. Em qualquer hipótese de abertura de chamados do CONTRATANTE junto à ALGAR TELECOM, excetuadas os casos previstos no item 6.1 acima, deverá a ALGAR TELECOM avaliar ou diagnosticar a ocorrência e contatar o CONTRATANTE, no prazo máximo de 2 (duas) horas, informando, se for o caso, o prazo para reparo/solução da falha ou problema apresentado.

7. TEMPO DE REPARO

7.1. O Tempo de Reparo é o tempo corrente desde a abertura do chamado pelo CONTRATANTE ou ocorrência de evento dos tipos Interrupção, até a completa resolução do problema ou reestabelecimento do fornecimento dos serviços.
7.2. O tempo de Reparo será computado por meio do sistema "CRM" da ALGAR TELECOM, o qual fará todas as tratativas dos chamados referentes às interrupções dos serviços, objeto do contrato.
7.3. Para os serviços que compõem a solução disponibilizada ao CONTRATANTE, objetivo da ALGAR TELECOM é reparar os serviços no tempo máximo de até 04 (quatro) horas por interrupção.

8. PENALIDADES EM CASO DE DESCUMPRIMENTO DE SLA

8.1. As Partes estabelecem, desde já, que as penalidades aplicadas por descumprimento dos parâmetros de qualidade indicados neste Acordo deverão ser revertidas ao CONTRATANTE na forma de crédito, o qual será concedido na Fatura até o segundo mês subsequente ao mês em que foi verificado o fato que deu origem à penalidade, sendo certo que tal crédito será efetuado com base no preço vigente no mês do crédito.
8.1.1 No caso de inoperância dos serviços causada por responsabilidade comprovadamente atribuível exclusivamente à ALGAR TELECOM, serão concedidos descontos conforme abaixo, limitado ao valor mensal do serviço, objeto dos Contratos:

D = I X P

Onde : D = desconto em R$ (reais) relativo aos serviços indisponíveis.
I = fator de indisponibilidade
P = preço mensal do serviço que ficou indisponível contratado.
8.1.2 Os preços mensais dos serviços são os constantes dos contratos firmados pelas partes.
8.1.3 Será considerado para apuração deste desconto, somente o valor mensal do serviço que ficou indisponível e não o valor mensal da solução global ALGAR TELECOM.
8.2. Reconhecem expressamente as partes que a limitação da responsabilidade conforme disciplinada no item 8.1. acima, decorre do mútuo interesse em manter os valores de eventual indenização devida por uma parte à outra em patamares proporcionais ao valor econômico do contrato.
8.3. A ALGAR TELECOM estabelece no item 8.1, os descontos referentes à prestação dos serviços caso haja descumprimento deste Acordo. Caso os níveis de serviço não sejam atingidos pela ALGAR TELECOM, o CONTRATANTE fará jus exclusivamente aos descontos previstos no item 8.1, que terão natureza de indenização compensatória e indenizatória pré-fixada.
8.4. Fica estabelecido, ainda, que todas as penalidades ora estabelecidas possuem caráter exclusivamente compensatório e indenizatório, nada mais tendo o CONTRATANTE a reclamar, razão pela qual a ALGAR TELECOM estará isenta de qualquer responsabilidade adicional, nos casos de descumprimento dos índices de qualidade previstos neste Acordo.

8.5. A ALGAR TELECOM não terá qualquer responsabilidade por falhas na prestação dos serviços ocasionadas, além de outras, por:
(i) caso fortuito ou eventos de força maior, tais como causas que estejam fora de sua capacidade de controle, incluindo ataques de vírus; eventos não previsíveis relacionados aos produtos, serviços e tecnologia utilizados pela ALGAR TELECOM;
(ii) imperícia, imprudência, condutas negligentes ou dolosas do CONTRATANTE;
(iii) falhas ou vícios nos equipamentos do CONTRATANTE e/ou irregularidades na respectiva operação pelo CONTRATANTE;
(iv) falhas, problemas de compatibilidade ou vícios em produtos ou serviços contratados pelo CONTRATANTE junto a terceiros;
(v) serviços por qualquer meio controlados pelo Poder Público, seus agentes e/ou quem suas vezes fizer;
(vi) desapropriação, ordens, proibições ou outros atos emanados pelo Poder Público, seus agentes e/ou quem suas vezes fizer.

9. PROCESSO DE REVISÃO

9.1. Sempre que houver alteração na solução ALGAR TELECOM para os serviços, seja ela ou não para melhoria nos indicadores de performance e tempo de resposta /solução, o contrato de SLA deverá ser revisado, sendo que eventuais alterações deverão ser devidamente formalizadas por meio de aditivo contratual.

DS EBDS DS FMSEH DS hugh

ANEXO III - CONDICOES ESPECIFICAS DO SERVIÇO INTERNET LINK

1. DESCRIÇÃO

O Internet Link é um serviço dedicado em alta velocidade para acesso à Internet, com característica de velocidade simétrica.
Este serviço é atendido por circuitos com características simétricas, utilizando fibra-óptica, modens HDSL ou até mesmo rádios digitais.
A simetria se refere ao sentido da comunicação *downstream* (central para o usuário) e *upstream* (usuário para central) opnde as velocidades *up* e *down* são iguais.
A conexão é permanente "*Always-on*" sem a necessidade de discar e aguardar e a informação é roteada de uma forma rápida e direta, com os mesmos atrasos (delay) possíveis.
O serviço Internet Link contém os seguintes componentes:
- ACESSO: É o circuito que interliga o endereço do cliente à rede da ALGAR TELECOM, e as configurações nesta rede, que permitem posteriormente a conexão do cliente ao backbone Internet;
- Porta: consiste na interligação do cliente ao backbone Internet. A velocidade da porta define a banda dedicada para tráfego IP.
Características de funcionamento: 1 Mbps, 2 Mbps, 3 Mbps, 4 Mbps, 5 Mbps, 6 Mbps, 7 Mbps, 8 Mbps, 9 Mbps, 10 Mbps, 11 Mbps, 12 Mbps, 13 Mbps, 15 Mbps, 16 Mbps, 17 Mbps, 18 Mbps, 19 Mbps, 20 Mbps, 25 Mbps, 30 Mbps, 34 Mbps, 35 Mbps, 40 Mbps, 45 Mbps, 50 Mbps, 60 Mbps, 70 Mbps, 80 Mbps, 90 Mbps, 100 Mbps, 150 Mbps, 155 Mbps, 200 Mbps, 250 Mbps, 300 Mbps, 350 Mbps, 400 Mbps, 450 Mbps, 500 Mbps, 600 Mbps, 622 Mbps, 700 Mbps, 800 Mbps, 900 Mbps, 1 Gbps, 1.5 Gbps, 2 Gbps, 2.5 Gbps, 3 Gbps, 3.5 Gbps, 4 Gbps, 4.5 Gbps, 5 Gbps, 5.5 Gbps, 6 Gbps, 6.5 Gbps, 7 Gbps, 7.5 Gbps, 8 Gbps, 8.5 Gbps, 9 Gbps, 9.5 Gbps, 10 Gbps, 15 Gbps, 20 Gbps, 25 Gbps, 30 Gbps, 35 Gbps, 40 Gbps, 45 Gbps, 50 Gbps, 55 Gbps, 60 Gbps, 65 Gbps, 70 Gbps, 75 Gbps, 80 Gbps, 85 Gbps, 90 Gbps, 95 Gbps, 100 Gbps.

Relatórios de trafego de Rede: A ALGAR TELECOM pode fornecer acessos para que o cliente possa verificar suas condições de tráfego e dimensionar suas necessidades de velocidade.
Números IP's (fixo e válido): Para o Internet Link com velocidade até 10 Mbps a quantidade de IP's é limitada em 4 IP's (3 utilizados pela Operadora para configurações e 1 disponível ao cliente), devendo o usuário migrar de velocidade caso precise de mais IP's. Para velocidades acima de 10 Mbps são liberados 8 IP's (3 utilizados pela Operadora para configurações e 5 disponíveis ao cliente).
Domínios: É de inteira responsabilidade do cliente, os registros de domínios bem como a manutenção dos mesmos, junto a FAPESP.

DS EBDS DS FMSEH DS hugh

ANEXO IV - CONDIÇÕES ESPECÍFICAS DOS SERVIÇOS DE SEGURANÇA – SERVIÇO ADICIONAL

Os serviços de Segurança consistem em monitor e tratar incidentes de Segurança em regime 24x7(vinte e quatro horas e sete dias por semana, incluindo feriados); por meio de um Centro de Operações de Segurança.

Trata-se de um serviço técnico em telecomunicações e TI, realizada de forma remota ou presencial, que tem por objetivo: manter o sigilo e a autenticidade das informações de interesse do usuário; protege-lo contra extravio de informações sigilosas; defender as informações que trafegam pela rede de telecomunicações de sofisticadas técnicas de ataque de hackers.

Para isto contamos com dois serviços distintos: Anti DDoS e Gerenciamento de Segurança.

Serviço Anti DDoS:

O serviço Anti DDoS consiste em monitoramento, detecção e tratamento dos seguintes ataques:

- Ataques de negação de serviço DoS e DDoS;
- Inundações de pacotes com SYN (SYN Flood) e UDP (UDP Flood);
- Ataque de volume a Servidores WEB, sistemas operacionais, sistemas de bancos de dados e Web Services;

A solução ainda retém os logs de alerta de alto impacto pelo período de 30 (trinta) dias, limitado a capacidade técnica da solução.

As regras iniciais serão definidas a partir de uma análise do perfil do cliente e das melhores práticas, sendo os ataques de alto impacto analisados prioritariamente;

Qualquer alteração em configuração da rede do cliente deverá esta ser informada ao Centro de Operações de Segurança da Algar Telecom, sob pena de ocorrerem ataques não identificados ou falsos alarmes, sem que estes causem dolo ou pena à Algar Telecom;

Demais informações e tratativas que por ventura forem necessárias para o bom desempenho do Serviço encontram-se registradas na Política de Privacidade de Uso disponível no portal *www.algartelecom.com.br*;

O serviço é oferecido em duas modalidades, a saber:

DDoS Automático

- Os incidentes de segurança deverão ser tratados pela equipe do Centro de Operações sem que haja necessidade de formalização com o cliente;
- As Alterações de configuração ou perfil do cliente no Anti DDoS Automático poderão ser feitas em acordo com as melhores práticas de segurança;
- O cliente terá acesso aos eventos de ataque por meio do Portal www.algartelecom.com.br;

DDoS Manual

- Os incidentes de segurança deverão ser tratados pela equipe do Centro de Operações e informados à equipe técnica do cliente por meio de contato previamente formalizado;
- As alterações de configuração ou perfil do cliente que contratou o Anti DDoS Manual deverão ser submetidas à avaliação de equipe técnica do cliente e aprovadas por este, sendo o contato por meio telefônico e/ou email.
- O cliente terá acesso aos eventos de ataque por meio de contato telefônico com o Centro de Operações de Segurança da Algar Telecom ou por meio do Portal www.algartelecom.com.br;

GERENCIAMENTO DE SEGURANÇA

O Gerenciamento de Segurança consiste em monitoramento do equipamento de segurança, UTM, de propriedade do cliente ou da Algar Telecom.

O serviço gerenciado é prestado remotamente em estrutura denominada SOC (*Security Operation Center*), composta por especialistas em redes de comunicação de voz e dados e em segurança da informação.

No SOC o equipamento é monitorado e os alarmes gerados pela ferramenta de gerenciamento são direcionados à equipe da Algar Telecom, que os analisa e gera uma resposta ao cliente, em um SLA de 4 horas úteis.

Ainda, mensalmente, é disponibilizado relatório de uso do equipamento conforme cada funcionalidade contratada.

As funcionalidades estão agrupadas em 3 grupos, a saber:

Funcionalidade 1: Gerência e Controle de Uso Interna (Firewall + VPN)

- Firewall → permite a elaboração de políticas de controle de acesso a redes/serviços de rede (email, ssh, http e etc);

- Balanceamento de Tráfego → utilizado para elaboração de políticas de roteamento, considerando roteamento estático, RIP ou BGP. Como exemplo de sua aplicação, podemos utilizar os protocolos de roteamento para controle de redundância entre filiais/saída para internet, alternando a saída de tráfego entre os links conforme disponibilidade dos mesmos.

- VPN Cliente → tecnologia utilizada para que o usuário final possa acessar o ambiente corporativo (interno do cliente) através de ambiente/rede externo (smartphone, computador ou outro dispositivo com acesso à internet).

Funcionalidade 2: Políticas de Segurança (App Control + Web Filtering + Anti Spam + Anti vírus)

Além dos serviços contidos na Funcionalidade 1, o cliente terá:

- App Control → Realização de controle de aplicações a partir de lista (black/white list) gerada de acordo com perfis/grupos de usuários previamente cadastrados (manualmente, por exemplo). Além disso, é gerada visibilidade de acesso às aplicações, largura de banda consumida, além do detalhamento de utilização de acordo com perfil de usuário/dispositivos cadastrados ;
- Web Filtering → Realização de controle de acesso ao ambiente web, a partir da lista de black/white list gerada de acordo com os perfis/grupos de usuários previamente cadastrados (manualmente, por exemplo). Além disso, é gerada visibilidade de acesso aos sites web, detalhamento de utilização de acordo com perfil de usuário/dispositivos cadastrados;
- Antivirus → Triagem do tráfego entrante nas redes do cliente, utilizando base de dados do Fabricante do equipamento para avaliação de possíveis malwares, spywares e demais ameaças geradas por hackers;
- Antispam → Triagem do tráfego de e-mail entrante na rede, utilizando base de dados d do Fabricante do equipamento, bloqueando entrada de e-mails detectadas como spam ou que contenham ameaças.

Funcionalidade 3: Controle de Invasão

Além dos serviços contidos nas Funcionalidades 1 e 2, o cliente terá:

- IPS (Intrusion Prevention System)→Tecnologia de segurança/prevenção de ameaças que examina os fluxos de tráfego de rede para detectar e prevenir exploits de vulnerabilidade. Os exploits de vulnerabilidade geralmente vêm na forma de entradas maliciosas em um aplicativo ou serviço alvo que os invasores usam para interromper e obter o controle sobre um aplicativo ou máquina.

A detecção baseada em assinatura se baseia em um dicionário de padrões (ou assinaturas) exclusivamente identificáveis no código de cada *exploit*. Quando um *exploit* é descoberto, sua assinatura é gravada e armazenada em um dicionário de assinatura que está sempre aumentando.

A detecção de anomalias estatísticas toma amostras aleatórias do tráfego de rede e as compara com um patamar de desempenho pré-calculado. Quando a amostra da atividade do tráfego de rede está fora dos parâmetros de um patamar de desempenho, o IPS realiza uma ação para resolver a situação.

Preço

Para definir o equipamento e os valores a serem cobrados mensalmente; as funcionalidades são combinadas de acordo com a banda do cliente e número de funcionários, desta combinação resulta-se no perfil e pacote mais aplicado ao cliente.

Cada um dos pacotes oferecidos, possuem licença que será renovada conforme cada período de contrato estabelecido. O cliente pagará pela Locação do Equipamento e Mensalidade do Serviço de Gestão.

Caso o cliente possua o equipamento e contrate a gerência do serviço para o mesmo, deverá escolher a funcionalidade mais adequada e pagará apenas pelo Serviço de Gestão. As licenças serão aplicadas por este time, mas deverão ser adquiridas pelo cliente.

O **CONTRATANTE** obriga-se a manutenção, conservação e reparação dos equipamentos necessários à prestação dos serviços de Gerenciamento de Segurança e que estiverem em sua posse, sendo de sua inteira responsabilidade zelar pelo seu bom funcionamento.

Quando o CONTRATANTE utilizar equipamento próprio ou contratado de terceiros que não diretamente da ALGAR TELECOM, será ele o único responsável pelos custos e necessárias manutenções preventivas/corretivas, bem como as consequências que estes equipamentos causarem direta ou indiretamente aos SERVIÇOS.

Para que a gestão se torne efetiva, a Algar Telecom deverá ser a única administradora do equipamento e qualquer adequação deve ser solicitada.

Demais informações e tratativas que por ventura forem necessárias para o bom desempenho do Serviço encontram-se registradas na Política de Privacidade de Uso disponíveis no portal www.algartelecom.com.br;

Relatórios Disponíveis para cada Funcionalidade:

Funcionalidade 1: Gerência e Controle de Uso Interna

Consumo de Banda
- ✓ Top 10 Usuários/origens por consumo de banda e sessões;
- ✓ Top 10 Destinos mais consumiram Banda;

Funcionalidade 2: Políticas de Segurança (além das informações contidas na Funcionalidade 1)

Consumo de Banda
- ✓ Top 10 Sites mais consumiram banda;
- ✓ Top 10 Aplicações por Banda;
- ✓ Top 10 Categorias aplicações por Banda.

Tráfego Bloqueado
- ✓ Top 10 Categorias web mais acessadas (tipos de sites, exemplo streaming, P2P);
- ✓ Top 30 Websites mais visitados (sites visitados pelo ambiente do cliente);
- ✓ Top 10 Bloqueio acesso por usuário (mostra os usuários mais bloqueados);
- ✓ Top 10 Categorias bloqueadas (mostra os tipos de sites mais bloqueados);
- ✓ Top 10 Sites bloqueados;
- ✓ Top 20 Aplicações Bloqueadas;

Funcionalidade 3: Controle de Invasão (além das informações contidas nas Funcionalidades 1 e 2)

Vulnerabilidades Identificadas
- ✓ Listagem Virus *Botnet* and *Spyware* and *Adware* identificados;
- ✓ Frequência de Bloqueio por Ataque de *Botnet*;
- ✓ Listagem de Máquinas infectadas com *Botnet*;
- ✓ Listagem de Aplicações de Alto Risco;
- ✓ Top 10 Vírus.

CONTRATO DE CONCESSÃO DE BENEFÍCIOS E OUTRAS AVENÇAS

DADOS CADASTRAIS DO CONTRATANTE

Razão Social/Nome:	**INSTITUTO BRASILEIRO DE GESTÃO HOSPITALAR IBGH**				
CNPJ:	**18.972.378/0009-70**				
Endereço (sede):	**Av. V-5**	Nº	**S/N**	Bairro	**Cidade Vera Cruz**
Cidade/Estado:	**Aparecida de Goiânia/GO**			Comp.	**Qd. A, Área Lt.001-E SALA 01**

DADOS DO SERVIÇO

Serviço:	**INTERNET LINK**	Velocidade:	**200 Mbps**
Valor Mensal:	**R$ 2.135,00**	Valor total:	**R$ 25.620,00**
Serviço:	**Gerenciamento de rede - NOC**	Velocidade:	-
Valor Mensal:	**R$ 89,00**	Valor total:	**R$ 1.068,00**
Serviço:	**Anti-DDoS**	Velocidade:	-
Valor Mensal:	**R$ 825,00**	Valor total:	**R$ 9.900,00**
Serviço:	**SOC AVANÇADO FG200-E**	Velocidade:	-
Valor Mensal:	**R$ 2.350,00**	Valor total:	**R$ 28.200,00**

BENEFÍCIOS E PRAZO DE PERMANÊNCIA MÍMINA

Benefício(s):	(i) SLA diferenciado de solução de incidentes; (ii) Investimentos específicos para atendimento à solução; (iii) Central de atendimento exclusivo para empresas.
Prazo de permanência:	**12 meses**

Pelo presente instrumento ("Contrato"), de um lado a da ALGAR MULTIMÍDIA S/A, prestadora de serviços de telecomunicações, inscrita no CNPJ n.º 04.622.116/0001-13, com sede na Rua José Alves Garcia, n.º 415, Bairro Brasil, na cidade de Uberlândia/MG, e ALGAR TELECOM S/A, prestadora de serviços de telecomunicações, inscrita no CNPJ n.º 71.208.516/0001-74, com sede na Rua José Alves Garcia, n.º 415, Bairro Brasil, na cidade de Uberlândia/MG por si ou por suas filiais, neste ato devidamente representadas, doravante denominadas "ALGAR TELECOM" e, de outro lado o CONTRATANTE acima, em conjunto ALGAR TELECOM e CONTRATANTE serão denominados "Partes" ou individualmente como "Parte".

Considerando que:

a. As Partes firmaram o CONTRATO/TERMO DE CONTRATAÇÃO para viabilizar a prestação pela ALGAR TELECOM ao CONTRATANTE do(s) Serviço(s) de Comunicação Multimídia ("Serviço");

b. A ALGAR TELECOM ofereceu ao CONTRATANTE benefício(s) para viabilizar e/ou implementar o Serviço e, em contrapartida o CONTRATANTE livremente concordou em permanecer vinculado a este Contrato pelo prazo e condições a seguir declinados.

c. O CONTRATANTE é uma pessoa jurídica de direito privado que exerce atividade empresarial e, utilizará o Serviço descrito neste instrumento para viabilizar a oferta e/ou prestação de seus serviços e produtos para os seus clientes finais.

d. O presente o presente Contrato rege-se pelas disposições da Lei nº 10.406 (Código Civil).

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente Contrato tem por objeto o ajuste de condições para concessão de certo(s) benefício(s) que será(ão) concedido(s) ao CONTRATANTE pela ALGAR TELECOM e, disciplinar a permanência mínima do CONTRATANTE ao presente Contrato.

CLÁUSULA SEGUNDA – DOS BENEFÍCIOS E PRAZO DE PERMANÊNCIA MÍNIMA

2.1. Para viabilizar a prestação do Serviço a ALGAR TELECOM concede ao CONTRATANTE o(s) benefício(s) descrito neste Contrato e, em contrapartida o CONTRATANTE compromete-se a permanecer vinculado a este Contrato pelo prazo de permanência mínima descrito no preâmbulo contratual. Após o decurso do prazo de vigência inicial descrito neste instrumento, o mesmo poderá ser renovado por meio de aditivo contratual.

2.2. Caso o CONTRATANTE proceda à denúncia, mediante envio de notificação por escrito à ALGAR TELECOM com 30 (trinta) dias de antecedência, solicite *downgrade* ou der causa à rescisão do Serviço durante o prazo de permanência mínima, ficará sujeito ao pagamento de multa correspondente a um percentual de 30% (trinta por cento) do valor das prestações vincendas, calculada com base no valor da prestação vigente no mês da extinção/cancelamento do Contrato.

2.2.1. O pagamento da multa estipulada neste item se dará de uma única vez, no prazo de até 30 (trinta) dias após o recebimento da comunicação da denúncia, *downgrade* ou rescisão contratual.

2.2.2. A multa referente à solicitação de *downgrade* corresponderá a um percentual de 30% (trinta por cento) calculada sobre a diferença entre as prestações inicialmente contratadas e as novas prestações ajustadas.

CLÁUSULA TERCEIRA – DAS DISPOSIÇÕES GERAIS

3.1. O CONTRATANTE declara ter ciência de que a ALGAR TELECOM realizou determinados investimentos e/ou realizou determinados custos para viabilizar a prestação do serviço objeto deste Contrato. Declara ainda que as penalidades previstas neste instrumento são estabelecidas em função de tais investimentos e/ou custos, não podendo, em caso de rescisão e/ou resilição, serem consideradas, para nenhum efeito, como ônus adicional, mas sim integrante da formatação do preço ora praticado.

3.2. O presente instrumento constitui título executivo extrajudicial, cobrável por meio de processo de execução específica, nos termos do Código de Processo Civil.

3.3. Se qualquer uma das disposições do presente Contrato for ou vier a tornar-se nula ou revelar-se omissa, tal nulidade ou omissão não afetará a validade das demais disposições deste Contrato.

3.4. As Partes declaram que: (i) leram este Contrato em sua íntegra e que a elas foi dada a oportunidade de esclarecer qualquer dispositivo e informação que não tivessem entendido; (ii) entendem os termos, condições e obrigações deste Contrato e concordam em estar legalmente submetidas por meio dele; (iii) não se verifica, na presente contratação, qualquer fato ou obrigação que possa vir a ser caracterizada como coação, estado de perigo ou lesão, conforme os arts. 151, 156 e 157 do Código Civil, respectivamente; (iv) estão cientes de todas as circunstâncias e regras que norteiam o presente negócio jurídico; e (v) as prestações a serem assumidas pelas Partes são reconhecidas por ambas como manifestamente proporcionais e tal proporcionalidade é decorrente de valores vigentes ao tempo em que é celebrado o presente negócio jurídico.

CLÁUSULA QUARTA – DO FORO

4.1. As Partes elegem o foro da comarca de Goiânia, Estado de Goiás para dirimir todas e quaisquer questões decorrentes e/ou relacionadas ao presente Contrato.

Goiânia, 11 de fevereiro de 2020.

Assinatura **CONTRATANTE:** DocuSigned by: Elinde Bento da Silva B6DEAC069BCD401...
Nome:
Cargo:

Assinatura **ALGAR TELECOM**: DocuSigned by: Federico Miguel Silva E Henriques 5093F2ED6C0A48E...
Nome:
Cargo:

DocuSigned by: Hugo Correia da Silva 179E982B515246C...
Nome:
Cargo:

TESTEMUNHAS:

Nome:
CPF: DocuSigned by: Ana Paula Freitas A43FE7416A744AA...

Nome:
CPF: DocuSigned by: Carlos Costa Pinto Neto D4F71B85D6CE4C4...

CONTRATO DE PRESTAÇÃO DE SERVIÇOS

Pelo presente contrato de prestação de serviço ("CONTRATO"), de um lado, o **CLIENTE**, pessoa física ou jurídica qualificado no Termo de Contratação (Anexo I) ao serviço ***SD-WAN***, doravante denominado **CLIENTE** e, de outro lado, **ALGAR TELECOM S/A**, prestadora de serviços de telecomunicações, inscrita no CNPJ nº 71.208.516/0001-74, com sede na Rua José Alves Garcia, nº 415, Bairro Brasil, na cidade de Uberlândia, Estado de Minas Gerais, e todas as suas filiais; **ALGAR MULTIMÍDIA S/A**, prestadora de serviços de telecomunicações, inscrita no CNPJ nº 04.622.116/0001-13, com sede na Rua José Alves Garcia, nº 415 - Mezanino, Bairro Brasil, na cidade de Uberlândia, Estado de Minas Gerais, e todas as suas filiais; **ALGAR SOLUÇÕES EM TIC S/A**, prestadora de serviços de telecomunicações, inscrita no CNPJ nº 22.166.193/0001-98, com sede na Rua José Alves Garcia, nº 415, Bloco A, Bairro Brasil, na cidade de Uberlândia, Estado de Minas Gerais, todas previamente qualificadas e, conforme aplicável, neste ato por seus representantes que abaixo assinam, doravante denominadas conjuntamente de **ALGAR TELECOM** e, em conjunto **CLIENTE** e **ALGAR TELECOM** serão denominados Partes ou individualmente Parte, celebram de comum acordo este "CONTRATO" que vigerá conforme as seguintes condições:

1. DO OBJETO

1.1. O presente **CONTRATO** tem por objeto a prestação pela **ALGAR TELECOM** ao seu **CLIENTE** de soluções e serviços complementares de conectividade.
1.2. A prestação desse serviço está condicionada à disponibilidade do serviço de acesso à internet independente da tecnologia.
1.3. A contratação de serviços de telecomunicações que servirão de insumo e suportarão o serviço de SD-WAN é de responsabilidade do CLIENTE, não se confundindo com o serviço de SD-WAN ora contratado.
1.4. Nos termos dos itens 1.1 e 1.2, fica registrado que o serviço de SD-WAN ora contratado configura serviço de valor adicionado, nos termos do artigo 61 da Lei nº 9.472, de 16 de julho de 1997.

2. DESCRIÇÃO E CARACTERÍSTICAS DO SERVIÇO

2.1. Este contrato refere-se ao Produto "*SD-WAN*", sendo que o CLIENTE declara conhecer as condições, prazos e preços referentes ao Serviço ora contratado, conforme descritos no Anexo I, bem como ter recebido informações sobre a Central de Atendimento da ALGAR TELECOM, devendo respeitar as condições descritas no site *www.algartelecom.com.br*
2.2. A prestação do serviço será através de equipamentos cedidos em comodato, bem como instalação/configuração e manutenção técnica; e segundo as condições estabelecidas neste contrato e no no site *www.algartelecom.com.br*.
2.3. As condições comerciais referentes às ofertas comercializadas pela ALGAR TELECOM estão dispostas no descritivo que estará disponível no site www.algartelecom.com.br.
2.4. Caso o CLIENTE solicite o cancelamento do serviço, automaticamente, será cobrado o valor *pro rata die*, sendo que os equipamentos serão recolhidos em prazo a ser acordado com o cliente.
2.5. O serviço destina-se ao uso exclusivo ao **CLIENTE**, sendo expressamente vedado a comercialização, distribuição, cessão gratuita ou onerosa, compartilhamento ou disposição dos sinais objeto do serviço e/ou dos equipamentos cedidos pela da **ALGAR TELECOM,** responsabilizando o **CLIENTE** penal e civilmente por eventuais descumprimentos da legislação aplicável ao serviço e ao CONTRATO.

3. DA INSTALAÇÃO E ATIVAÇÃO DO SERVIÇO

3.1. O aceite demonstrado por meio escrito, telefônico e/ou eletrônico do **CLIENTE** com relação ao serviço, expressa a sua anuência aos termos e condições da prestação do serviço pela **ALGAR TELECOM.**
3.2. Mediante prévia autorização, a **ALGAR TELECOM incluirá** as informações cadastrais do **CLIENTE** no seu banco de dados, o qual a partir de então, passará a receber informações sobre lançamentos, ofertas especiais e promoções da **ALGAR TELECOM** ou de terceiros.
3.3. A instalação dos serviços poderá ser feita pela ALGAR TELECOM, ou por terceiro autorizado pela ALGAR TELECOM, sujeito a cobrança e viabilidade técnica.
3.4. Caso o CLIENTE adquira o equipamento de terceiros, a ALGAR TELECOM não se responsabiliza pela instalação e manutenção deste equipamento, sendo responsável somente pela prestação do serviço SD-WAN.

4. DO PREÇO E FORMA DE PAGAMENTO

4.1. Pelo serviço prestado o CONTRATANTE pagará mensalmente à ALGAR TELECOM, por meio de nota fiscal/fatura de prestação de serviços, o valor mensal correspondente ao Serviço que expressamente contratar junto à ALGAR TELECOM.
4.2. O não recebimento da nota fiscal/fatura de prestação do serviço no endereço indicado pelo CONTRATANTE não o isenta do pagamento dos serviços prestados pela ALGAR TELECOM.
4.3. Qualquer alteração na carga tributária incidente sobre o Serviço poderá implicar no aumento ou diminuição dos preços acordados.
4.4. Para os serviços descritos será cobrada manutenção mensal, sendo que o pagamento de tal manutenção garante a prestação do serviço, bem como a substituição dos equipamentos durante o período de contratação, mediante comprovação de defeito, desde que não seja por uso indevido do equipamento.
4.5. Durante o período que o cliente estiver usufruindo o serviço e pagando a manutenção mensal, as reconfigurações e/ou atualizações do equipamento, serão de responsabilidade exclusiva da Algar Telecom.
4.6. Nos casos em que haja a gestão compartilhada dos equipamentos, em virtude da natureza da prestação dos serviços, o CLIENTE deve comunicar à ALGAR TELECOM sobre a necessidade de intervenção nos equipamentos cedidos, de acordo com o descrito no Anexo II.

5. DA INTERRUPÇÃO DO SERVIÇO

5.1. O **CLIENTE** entende e concorda que o serviço estará sujeito a períodos de eventual indisponibilidade, seja para manutenção programada (preventiva), ou não programada (emergencial), dificuldades técnicas, ambientais (incluindo chuvas, vendavais etc.) e/ou outros fatores fora do controle da **ALGAR TELECOM**.

DS EBDS DS FMSEH DS hugh

5.2. Caso o cliente opte pelo cancelamento do serviço, a qualquer momento, automaticamente serão também canceladas as garantias e manutenções relacionadas.

6.1. DA VIGÊNCIA DO SERVIÇO E EXTINÇÃO CONTRATUAL

6.1. A vigência deste CONTRATO iniciará com a instalação do serviço e vigorará por prazo descrito no ANEXO I.
6.1.1. Caso qualquer uma das PARTES não tenha interesse na prorrogação do SERVIÇO, deverá comunicar a outra parte por escrito até a data de seu termo. Após o decurso do prazo de vigência inicial descrito neste instrumento, o mesmo poderá ser renovado por meio de aditivo contratual.
6.1.2. Caso o CONTRATANTE proceda a denúncia, mediante envio de notificação por escrito a ALGAR TELECOM, solicite downgrade ou der causa a rescisão e/ou interrupção do SERVIÇO, ficará sujeito ao pagamento de multa compensatória correspondente a um percentual de 30% (trinta por cento) do valor das prestações vincendas, calculada com base no valor da prestação vigente no mês da extinção contratual.
6.1.3. O pagamento da multa estipulada no item acima se dará de uma única vez, depois de transcorridos 30 (trinta) dias da comunicação da denúncia, downgrade ou rescisão contratual.
6.1.4. A multa referente a solicitação de downgrade corresponderá a um percentual de 30% (trinta por cento) calculada sobre a diferença entre as prestações inicialmente contratadas e as novas prestações ajustadas.
6.2. O presente contrato poderá ser extinto/encerrado nas seguintes hipóteses:
6.2.1. Solicitação pelo **CLIENTE** que não mais tiver interesse na continuidade da prestação do serviço, desde que obedecidas as condições comerciais;
6.2.3. Quando o endereço indicado pelo **CLIENTE** na ordem de serviço não apresentar as condições técnicas e/ou de segurança necessárias à ativação ou prestação do serviço ou ainda, quando não houver autorização condominial para sua instalação e/ou manutenção, sem ônus adicionais a quaisquer das Partes.
6.2.4. Rescisão, por qualquer das Partes, decorrente do descumprimento de obrigação contratual.
6.2.5. Uso indevido do serviço pelo **CLIENTE**, com ou sem adulteração dos equipamentos, ou por qualquer outro meio que lhe permita fruir do serviço de forma diversa da originalmente contratada com a **ALGAR TELECOM**.
6.2.6. Pela **ALGAR TELECOM**, mediante o envio de correspondência ao **CLIENTE**, com pelo menos 30 (trinta) dias de antecedência, sem que caiba qualquer indenização, sem prejuízo da aplicação da regulamentação específica do serviço.
6.2.7. Pedido de falência ou a decretação de falência de qualquer uma das Partes, ou ainda, qualquer evento análogo que caracterize o seu estado de insolvência, incluindo acordo com credores e o processamento da recuperação extrajudicial.
6.2.8. Caso fortuito ou força maior que impeça qualquer das Partes de cumprir suas obrigações, se o impedimento perdurar por pelo menos 30 (trinta) dias.

7. DIREITOS E OBRIGAÇÕES DO CLIENTE

7.1. São obrigações do **CLIENTE**:
7.1.1. Utilização adequada do **SERVIÇO** e dos **EQUIPAMENTOS** fornecidos em comodato pela **ALGAR TELECOM** em conformidade com os requisitos técnicos, procedendo com lealdade e boa-fé;
7.1.2. Prestação das informações que lhe forem solicitadas relacionadas à fruição do **SERVIÇO** e colaboração para sua adequada prestação, obrigando-se a manter seus dados cadastrais atualizados;
7.1.3. Cumprimento regular das obrigações assumidas neste **CONTRATO**;
7.1.4. Pagamento pela prestação dos serviços na forma contratada;
7.1.5. Prestar informações necessárias para o melhor cumprimento deste Contrato;
7.1.6. Exigir a observação das normas emanadas pelos órgãos de fiscalização e controle, e
7.2. São direitos do **CLIENTE**:
7.2.1. Acesso aos **SERVIÇOS** com padrões de qualidade e regularidade adequados à sua natureza em sua área de prestação do serviço, conforme condições contratadas;
7.2.2. Respeito à sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais;
7.2.3. Adequada prestação do **SERVIÇO** que satisfaça às condições de regularidade, respeito no atendimento, cumprimento de normas e prazos procedimentais;
7.2.4. Acesso gratuito para encaminhamento de demandas, reclamações, solicitações de informações, serviços e sugestões;

8. DAS OBRIGAÇÕES DA CONTRATANTE

8.1. Prestar serviços, dentro dos padrões de qualidade e eficiência exigidos para o serviço e nos dispositivos legais e convencionais impostos.
8.2. Manter no curso do contrato a sua regularidade fiscal e qualificação técnica exigível para o desempenho do objeto contratual.
8.3. Sanar eventuais irregularidades ou correções apontadas pela CONTRATANTE quanto à apresentação de relatórios e/ou de cada etapa dos serviços.
8.4. Impedir o acesso à unidade de pessoa que não seja membro de seu corpo técnico com o fim de trabalhar, estagiar ou realizar qualquer atividade similar.

9. DA MUDANÇA DE ENDEREÇO OU PONTO DE INSTALAÇÃO PRINCIPAL

9.1. Para os casos de mudanças de endereço, nas quais o cliente remunera pelo serviço de manutenção mensal, a responsabilidade de instalação no novo endereço será da Algar Telecom.
9.2. Não sendo possível a prestação do serviço no endereço de transferência, por razões de ordens técnicas, comerciais ou fora da área de atuação da ALGAR TELECOM, o presente contrato será resilido mediante solicitação do CLIENTE, o serviço de manutenção mensal, sendo cobrado o valor *pro rata die*.
9.3. O CONTRATANTE terá o serviço de disponível para degustação pelo período de 30 (trinta) dias corridos, contados a partir de sua ativação. Até o 29º dia o CONTRATANTE poderá solicitar a desconexão do serviço, com isenção do pagamento da primeira mensalidade.

9.3.1. Após o período de 30 (trinta) dias da ativação dos serviços, a CONTRATADA poderá, em caso de pedido de cancelamento, exigir o cumprimento das cláusulas desse contrato.
9.3.2. O CONTRATANTE não poderá alterar as características do serviço contratado durante este período, tais como, mas não se limitando a: tipo de acesso, banda e endereço de instalação.
9.3.3. Inobstante o disposto no item 8.3., os direitos e obrigações gerais serão aplicáveis e exigíveis pelas Partes desde a ADESÃO à PROPOSTA, inclusive os referentes à resilição, à rescisão ou à renúncia.

10. DAS OBRAS CIVIS E AUTORIZAÇÕES CONDOMINIAIS

10.1. Caso a ativação do serviço dependa da execução de obras civis e/ou autorizações condominiais por parte do **CLIENTE**, este deverá providenciá-las por conta própria e às suas expensas, arcando com todos os custos decorrentes da contratação de mão-de-obra e aquisição de material, bem como se responsabilizando pelas consequências da eventual ausência de autorização.

11. DAS DISPOSIÇÕES FINAIS

11.1. Esse serviço não tem relação com a garantia de entrega da velocidade contratada no acesso de internet. As condições de prestação do serviço de acesso à internet são as contratadas pelo cliente com o fornecedor de serviços internet, não cabendo à ALGAR TELECOM nenhuma responsabilidade relativa à este serviço.
11.2. Poderá a **ALGAR TELECOM ceder** ou transferir os direitos e obrigações oriundos do presente CONTRATO para qualquer uma das empresas do mesmo grupo econômico ou em função de reestruturação societária, fusão, cisão ou incorporação, nos termos da regulamentação.
11.3. A senha de acesso a sistemas disponibilizada pela **ALGAR TELECOM** ao **CLIENTE** é de responsabilidade exclusiva deste, isentando a **ALGAR TELECOM** de qualquer responsabilidade pelo seu uso, sendo responsabilidade do **CLIENTE**, assumir todo ônus que possam surgir em virtude da má utilização e guarda.
11.4. Toda solicitação estará sujeita a um estudo sobre a viabilidade técnica, sendo que somente serão considerados contratados os serviços após a constatação de viabilidade técnica.
11.5. Para o esclarecimento de dúvidas relacionadas à prestação do serviço e acesso à tabela de valores, a **ALGAR TELECOM** disponibiliza ao **CLIENTE** sua Central de Atendimento, acessível por meio do telefone 0800 942 1212, por meio do *site* www.algartelecom.com.br, atendimento pessoal, de forma consultiva e ainda, possibilidade de envio de correspondência para o endereço descrito no preâmbulo contratual.
11.6. São partes integrantes e indissociáveis a este termo os anexos I (DADOS DA CONTRATAÇÃO) e II (TERMO DE RESPONSABILDIADE ADITIVO AO CONTRATO DE PRESTAÇÃO DO SERVIÇO) que trazem informações indispensáveis à presente contratação.
11.7. A CONTRATADA por si e por seus sócios, administradores, gestores, representantes legais, empregados, prepostos e subcontratados ("Colaboradores"), se compromete a adotar os mais altos padrões éticos de conduta na condução dos seus negócios e não pagar, prometer ou autorizar o pagamento de qualquer valor ou oferecer qualquer tipo de vantagem indevida direta ou indiretamente, a qualquer Funcionário Público ou a terceira pessoa, bem como garante que não emprega e não empregará, direta ou mediante contrato de serviços ou qualquer outro instrumento, trabalho escravo, trabalho infantil.
11.8. A CONTRATADA declara, sob as penas da lei, que não esteve envolvida com qualquer alegação de crime de lavagem de dinheiro, delito financeiro, financiamento de atividades ilícitas ou atos contra a Administração Pública, incluindo, mas não se limitando a corrupção, fraude em licitações, suborno ou corrupção e que durante a prestação dos serviços ora avençado, cumprirá com todas as leis aplicáveis à natureza dos serviços contratados, em especial a Lei de Improbidade Administrativa e Lei Brasileira Anticorrupção.
11.9. Fica acordado entre as partes que qualquer documentação administrativa ou judicial somente terá validade se direcionada à CONTRATANTE, para o seguinte endereço: Rua Av. Areião, Qd. 17, Lt. 23, CEP: 74820-370, Setor Pedro Ludovico, Goiânia – Goiás.

12. DO FORO

12.1. Fica eleito o foro da comarca onde o serviço foi contratado, para dirimir toda e qualquer dúvida oriunda do presente Contrato.

Goiânia, 11 de fevereiro de 2020.

Assinatura **CONTRATANTE:** DocuSigned by: Elinde Bento da Silva B6DEAC069BCD401...
Nome:
Cargo:

Assinatura **ALGAR TELECOM**: DocuSigned by: Federico Miguel Silva E Henriques 5093F2ED6C0A48E...
Nome:
Cargo:

DocuSigned by: Hugo Correia da Silva 179E982B515246C...
Nome:
Cargo:

TESTEMUNHAS:

Nome:
CPF: DocuSigned by: Ana Paula Freitas A43FE7416A744AA...

Nome:
CPF: DocuSigned by: Carlos Costa Pinto Neto D4F71B85D6CE4C4...

ANEXO I
DADOS DA CONTRATAÇÃO

DADOS DO CONTRATANTE:

Nome / Razão Social: **INSTITUTO BRASILEIRO DE GESTÃO HOSPITALAR IBGH**			
CPF / CNPJ: **18.972.378/0009-70**		I.E.:	
Endereço: **Av. V-5, S/N, Qd. A, Área Lt.001-E SALA 01**			
Bairro: **Cidade Vera Cruz**	CEP: **74936-600**	Cidade: **Aparecida de Goiânia**	UF: **GO**

CONTATO TÉCNICO:

Nome	**Jefferson Tadeu**
Telefone	**(62) 98406-1362**

DADOS DE FATURAMENTO

Nome / Razão Social: **INSTITUTO BRASILEIRO DE GESTÃO HOSPITALAR IBGH**			
CPF/CNPJ: **18.972.378/0009-70**			
Endereço: **Av. V-5, S/N, Qd. A, Área Lt.001-E SALA 01**			
Bairro: **Cidade Vera Cruz**	CEP: **74936-600**	Cidade: **Aparecida de Goiânia**	UF: **GO**

DADOS CONTRATUAIS

Prazo Contratual	**12 meses**
Fator de Correção	**IGP-M**

DADOS DE INSTALAÇÃO

Endereço: **Av. V-5, S/N, Qd. A, Área Lt.001-E SALA 01**			
Bairro: **Cidade Vera Cruz**	CEP: **74936-600**	Cidade: **Aparecida de Goiânia**	UF: **GO**

DADOS DO PRODUTO

Nº Serviço	Produto / Componente	Prazo de Execução (Dias úteis)	Custo de Instalação	Custo Mensal (Sem Impostos)	Custo Mensal (Com Impostos)
A definir	**SDWAN**	**30 DIAS**	**ISENTO**	**R$ 1.428,00**	**R$ 1.600,00**

TOTAIS

Total do custo mensal recorrente	**R$ 1.600,00**
Total do custo não recorrente	**R$ 0,00**

Goiânia, 11 de fevereiro de 2020.

Assinatura **CONTRATANTE:** DocuSigned by: Elinde Bento da Silva B6DEAC069BCD401...
Nome:
Cargo:

Assinatura **ALGAR TELECOM:** DocuSigned by: Federico Miguel Silva E Henriques 5093F2ED6C0A48E...
Nome:
Cargo:

DocuSigned by: Hugo Correia da Silva 179E982B515246C...
Nome:
Cargo:

TESTEMUNHAS:

Nome:
CPF: DocuSigned by: Ana Paula Freitas A43FE7416A744AA...

Nome:
CPF: DocuSigned by: Carlos Costa Pinto Neto D4F71B85D6CE4C4...

ANEXO II

TERMO DE RESPONSABILIDADE ADITIVO AO CONTRATO DE PRESTAÇÃO DO SERVIÇO

CONTRATANTE
Razão social: **INSTITUTO BRASILEIRO DE GESTÃO HOSPITALAR IBGH**
CNPJ: **18.972.378/0009-70**
Endereço: **Av. V-5, S/N, Qd. A, Área Lt.001-E SALA 01, Cidade Vera Cruz, Aparecida de Goiânia/GO.**
CONTRATADA
Razão social: **ALGAR SOLUÇÕES S/A / ALGAR MULTIMIDIA S/A**
CNPJ: 04.622.116/0001-13 / 22.166.193/0001-98
Endereço: Rua José Alves Garcia, 415, mezanino, bairro Brasil, na cidade de Uberlândia, estado de Minas Gerais.

Pelo presente instrumento, as PARTES acima qualificadas, resolvem de comum acordo, firmar o compromisso descrito abaixo:

CLÁUSULA PRIMEIRA – DA GESTÃO COMPARTILHADA

1. A partir da data de assinatura deste instrumento a CONTRATANTE passará a possuir a gestão compartilhada do EQUIPAMENTO SD-WAN contratado, sendo capaz de realizar quaisquer alterações na configuração do mesmo.

1.1. A CONTRATANTE declara que seus prepostos e contratados possuem conhecimento e capacidade técnica para a utilização correta e adequada da operação do serviço contratado.

1.2. A CONTRATANTE declara ciência de que será administradora capaz de executar rotinas e alterar as configurações do serviço, e que consequentemente possuirá permissão para incluir, alterar, excluir regras de segurança do serviço contratado, em conjunto com a CONTRATADA.

CLÁUSULA SEGUNDA – DAS RESPONSABILIDADES

2. A partir da assinatura deste instrumento a CONTRATANTE concorda que quaisquer eventuais alterações indevidas, falhas de segurança, danos ou riscos ocasionados pela má gestão do serviço de segurança por parte da CONTRATANTE, são de sua única e exclusiva responsabilidade.

2.1 Do mesmo modo, a CONTRATANTE concorda em isentar completamente a CONTRATADA de toda e qualquer responsabilidade por quaisquer alterações que a CONTRANTE execute no serviço de segurança que resultem em danos, perdas, falhas ou riscos de segurança, a si ou a terceiros, ocasionados por sua utilização indevida.

DS EBDS DS FMSEH DS hugh

TERMO DE REFERÊNCIA

1. OBJETO:

1.1 Contratação de empresa especializada na prestação de serviços de internet, para o Hospital Municipal de Aparecida de Goiânia CNES 9680977, de acordo com a Resolução de Diretoria Colegiada – RDC nº 63, de 25 de novembro de 2011, do Ministério da Saúde – MS, dispõe sobre os Requisitos de Boas Práticas de Funcionamento para os Serviços de Saúde, e nos termos do Contrato de Gestão 1095/2018 firmado entre o CONTRATANTE e o Município de Aparecida de Goiânia e a Secretaria Municipal de Saúde / Fundo Municipal de Saúde.

1.2 O presente objeto refere-se a contratação de empresa especializada que promova solução em serviços de telecomunicações com capacidade para prover tráfego de dados das aplicações corporativas da unidade hospitalar HMAP, tráfego de voz e imagens, videoconferência e acesso à Internet. Esses serviços serão prestados para interligação de unidade com a rede mundial de computadores e segurança da informação como previsto na lei geral de proteção de dados a LGPD.-

2. JUSTIFICATIVA

2.1. Tendo em vista a necessidade de garantir a continuidade dos serviços da unidade hospitalar essa nova aquisição deve ser contratada junto a outra operadora para garantir a continuidade dos serviços prestados a comunidade.

2.2. Dado a expansão dos serviços prestados e a implantação do serviço de exames de imagens que iniciou nesta unidade faz-se necessário garantirmos a qualidade e continuidade do trafego com segurança.

3. Planilha de Formação de Preços

Item	Descrição e Especificações	Unidade de Medida	Quantidade	Preço Unitário (R$)	Preço Total (R$)
1	Serviço de instalação de enlace dedicado à Internet.	Instalação	1		
2	Fornecimento de link de acesso dedicado à Internet na velocidade de 200 Mbps.	Meses	12		
3	Prestação de serviços de gerenciamento proativo do(s) link(s).	Meses	12		
4	Serviço de proteção contra ataques volumétricos de negação de serviços do tipo DDoS.	Meses	12		
5	Serviço de instalação e configuração da solução de segurança.	Instalação	12		
6	Fornecimento de solução de segurança do tipo NGFW.	Meses	12		
Total					

4. FUNDAMENTAÇÃO LEGAL:

4.1. Melhoria da qualidade dos serviços prestados ao cidadão e redução nos tempos de atendimento ao usuário.

4.2. Essa contratação agregará o serviço de filtros de dados que nos garante uma maior segurança nos dados trafegados.

5. DEFINICÕES:

5.1. Backbone: infraestrutura de interligação de uma rede, constituída de roteadores de borda do provedor e roteadores de núcleo, bem como os circuitos que existam entre eles.

5.2. ANATEL: Agência Nacional de Telecomunicações.

5.3. CPE (de Customer Premises Equipment): é um termo técnico muito utilizado por operadoras de telecomunicações e fornecedores de serviços de comunicação. Se trata do equipamento instalado dentro das instalações do cliente para prestação do serviço pela Operadora.

5.4. DNS: de *Domain Name System*, ou "Sistema de Nomes de Domínios". Trata-se, de servidores que armazenam listagens de domínios e seus respectivos endereços IPs. são os responsáveis por localizar e traduzir para números IP os endereços dos sites utilizados nos navegadores.

5.5. HTTP: O *Hypertext Transfer Protocol*, é um protocolo de comunicação utilizado para sistemas de informação de hipermídia, distribuídos e colaborativos. Ele é a base para a comunicação de dados da World Wide Web. Hipertexto é o texto estruturado que utiliza ligações lógicas entre nós contendo texto.

5.6. IP (de Internet Protocol): é um protocolo de comunicação usado para encaminhamento dos dados entre equipamentos em rede, utilizando endereços alocados em cada um dos elementos da mesma (endereços IP).

5.7. Last Mile ou Última Milha: circuito dedicado entre o roteador de borda do provedor e o roteador ou switch existente nas dependências do cliente.

5.8. MTTR: de *Mean Time to Repair* é um indicador de desempenho usado na manutenção para indicar o Tempo Médio Para Reparo de algum equipamento, componente, máquina ou sistema.

5.9. Router ou Roteador: equipamento tipicamente utilizado para fazer a interface entre uma rede local e uma rede de telecomunicações. É usado também nos nós de uma rede para processar roteamento do tráfego IP.

5.10. SLA: *Service Level Agreement*, que é traduzido em português por ANS (Acordo de Nível de Serviço). Refere-se à especificação, em termos mensuráveis e claros, de todos os serviços que o contratante pode esperar do fornecedor na negociação.

5.11. SNMP (Simple Network Management Protocol): protocolo de gerenciamento usado normalmente em redes IP.

5.12. DDoS (Distributed Denial of Service): é um ataque distribuído, o qual pode estar vinculado à milhares de computadores com interesse malicioso.

5.13. NGFW (Next Generation Firewall): um sistema de segurança baseado em hardware ou software que está habilitado a detectar e bloquear ataques sofisticados por reforçar políticas de segurança na camada de aplicação, camada 7 no modelo OSI.

6. ESPECIFICAÇÕES TÉCNICAS DO OBJETO:

6.1. REQUISITOS GERAIS

6.1.1. Contratação de empresa especializada para o fornecimento de acesso à Rede Mundial de Internet com 100% de garantia de banda downstream e upstream, full-duplex, com conectividade em protocolos IPv4 e IPv6.

6.1.2. Toda a infraestrutura de rede, acesso e CPE da CONTRATADA deverão ser dimensionadas e preparadas para suportar a totalidade do serviço.

6.1.3. A CONTRATADA deverá reservar os canais de comunicação e as portas de acesso à sua infraestrutura para uso exclusivo da CONTRATANTE, não sendo admitido o compartilhamento desses recursos com outro de seus clientes ou usuários

6.1.4. O acesso referido no item anterior deverá ser provido por meio de backbone próprio da prestadora de serviço.

6.1.5. Os equipamentos da CONTRATADA utilizados em toda a solução deverão ser novos e compatíveis com ambientes corporativos ou institucionais modernos.

6.1.6. A CONTRATADA obriga-se e se responsabiliza a prestar o serviço objeto da licitação, por meio de mão de obra especializada e devidamente qualificada, necessário à completa e perfeita execução dos serviços, em conformidade com as especificações do Termo de Referência.

6.1.7. Será de responsabilidade da CONTRATANTE o fornecimento de energia elétrica para alimentação dos equipamentos nas dependências das unidades, o aterramento da rede elétrica e a climatização das dependências.

6.2. CARACTERÍSTICAS DO LINK INTERNET

6.2.1. Fornecer e instalar link de Internet na taxa de 200Mbps dedicado.

6.2.2. A CONTRATADA deverá disponibilizar 04 endereços IPV4 e 04 endereços IPv6 fixos e válidos para provimento da solução de Internet.

6.2.3. A conexão entre o CPE da CONTRATADA e o equipamento da CONTRATANTE deverá ser realizada através de interface Gigabit Ethernet 1000BASE-TX.

6.2.4. A CONTRATADA poderá utilizar acessos de terceiros como última milha, sendo de inteira responsabilidade da CONTRATADA o cumprimento dos SLAs especificados 99.5%.

6.2.5. A velocidade do link do serviço entregue à CONTRATANTE deverá ser correspondente a 100% da banda contratada.

6.2.6. O acesso físico (conexão entre o ponto de presença da CONTRATADA e os equipamentos de comunicação de dados da CONTRATADA instalados nas dependências da CONTRATANTE) deverá ser realizado exclusivamente por meio de fibra óptica, sendo vedada a utilização de qualquer outra tecnologia de acesso.

6.2.7. O serviço de Internet deverá ser entregue em rede roteada, utilizando protocolos de camada 3, com SLA 99,5% de disponibilidade e MTTR de vinte quatro (24) horas.

6.2.8. Disponibilizar serviço de Domain Name Resolution (DNS) da CONTRATADA, capaz de resolver direta e reversamente endereços de Internet, para registro no servidor DNS primário.

6.2.9. Ser monitorado em regime 24x7 por centro de monitoração da CONTRATADA, sendo responsável pela administração e gerência de equipamentos e links de comunicação de dados, manutenção dos níveis mínimos de serviços exigidos e prevenção e recuperação de falhas de serviço.

6.2.10. Disponibilizar informações sobre os serviços de acesso à Internet por meio de um portal de monitoramento, com acesso restrito, utilizando protocolo seguro (HTTPS), contendo estatísticas de desempenho e de disponibilidade do acesso.

6.2.11. Possibilitar que a equipe técnica da CONTRATANTE realize consultas no portal de monitoramento, bem como visualize relatórios das informações de desempenho dos serviços contratados

6.2.12. A CONTRATADA não poderá:

a) Implementar nenhum tipo de filtro de pacotes que possa incidir sobre o tráfego originado ou destinado à CONTRATANTE, a menos que tenha expressa concordância com esta.

b) Implementar nenhum tipo de cache transparente, a menos que tenha expressa concordância da CONTRATANTE.

6.3. CARACTERÍSTICAS DO ROTEADOR

6.3.1. O roteador a ser instalado no ambiente da CONTRATANTE deverá ter no mínimo as seguintes características técnicas:

a) O equipamento e seus módulos e softwares não deverão constar em nenhuma lista do fabricante com as situações de "End-of-Sale", "End-of-Order", "End-of-Life" ou

"End-of-Support".

b) Deve possuir no mínimo quatro (04) interfaces Gigabit Ethernet padrão 1000BASE-TX.

c) Possuir protocolo SNMP habilitado com acesso de leitura.

d) Deve implementar os protocolos de roteamento RIP, OSPFv2, OSPFv3 e BGP-4.

e) Deve possuir suporte nativo ao protocolo IPv6.

f) Deve possuir suporte ao protocolo Netflow v9 ou superior.

g) Deve possuir suporte ao protocolo 802.1q.

h) Deve possuir suporte aos protocolos Telnet e SSHv2.

i) Deve possuir gerenciamento local através de uma porta console, sendo que todos os cabos e adaptadores necessários para o gerenciamento através da porta console deverão ser fornecidos pela CONTRATADA de forma a propiciar o gerenciamento do roteador a partir de uma porta USB.

j) Deverá ser disponibilizado para a CONTRATANTE com o último release de software estável disponibilizado pelo fabricante, capaz de atender a todos os requisitos acima, incluindo o suporte à atualização do referido software durante o período de vigência do contrato.

k) Deve ser montável em rack padrão EIA-310 com largura padrão 19" ocupando no máximo 1U de altura.

6.4. CARACTERÍSTICAS DO SERVIÇO Anti DDoS

6.4.1. A CONTRATADA deverá prover, no âmbito do serviço de segurança do link de Internet, uma solução para identificação, tratamento e mitigação transparente de ataques volumétricos do tipo negação de serviço distribuído (DDoS – Distributed Denial of Service).

6.4.2. A CONTRATADA deve possuir infraestrutura de mitigação própria com capacidade para conter ataques de grande volume, sendo eles de origem nacional ou internacional. Deverá possuir pelo menos 2 (dois) centros de limpeza, cada um com capacidade de mitigação de 40 Gbps (quarenta gigabits por segundo).

6.4.3. A CONTRATADA deverá disponibilizar em seu backbone, proteção contra ataques volumétricos de negação de serviço, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DDoS (Distributed Denial of Service).

6.4.4. A CONTRATADA deverá prover o serviço de mitigação sem limitação de tempo de duração do ataque e com quantidade ilimitada de eventos de ataque ao longo da vigência contratual.

6.4.5. O ataque deve ser mitigado separando o tráfego legítimo do tráfego malicioso, de

modo que os serviços de Internet providos pelo cliente continuem disponíveis.

6.4.6. A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos.

6.4.7. Em casos de ataques não detectados pela solução, quando identificados pela CONTRATANTE, deverão ser mitigados imediatamente pelas CONTRATADA após a abertura de chamado através da Central de Atendimento sempre como um chamado com Prioridade Máxima, e deverá realizá-la, sem nenhum ônus ao CONTRATANTE.

6.4.8. O serviço deve prover suporte à mitigação automática de ataques, utilizando múltiplas técnicas incluindo, mas não se restringindo a: White Lists, Black Lists, limitação de taxa de tráfego, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP, NTP e DNS, bloqueio por localização geográfica de endereços IP.

6.4.9. A CONTRATADA deve realizar a detecção de ataques utilizando-se dos recursos mais atuais para detecção de ataques de negação de serviço, tais como análise estatística de tráfego, padrões predefinidos para bloqueios de ataques, correlacionamento com ataques que estejam ocorrendo simultaneamente em outras partes do mundo e atualização para detecção de ataques de negação de serviço desconhecidos.

6.4.10. O serviço deve prover também análise de tráfego baseado em reputação de endereços IP, possuindo base de informações própria, que pode ser gerada durante a filtragem de ataques e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.

a) O serviço deve prover mecanismos capazes de detectar e migar todos e quaisquer ataques de DDoS que façam o uso não autorizado de recursos de rede, tanto para Ipv4 Ataques de inundação (Bandwidth Flood), Floods de UDP, TCP e ICMP.

b) Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets.

c) Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP.

d) Ataques provenientes de Botnets, Worms e que utilizam falsificação de endereços IP origem (IP Spoofing).

e) Ataques à camada de aplicação, incluindo protocolos HTTP, DNS, NTP, dentre outros.

f) O serviço deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pela CONTRATADA.

g) O serviço deve permitir a configuração de níveis diferenciados de proteção por grupo

de hosts ou subnets.

h) O serviço deve ser capaz de bloquear tráfego baseado em assinaturas em até 15 minutos.

i) O serviço deve ser capaz de analisar e aprender o comportamento do tráfego para criar automaticamente parâmetros de bloqueio (Limite de conexão HTTP, TCP, UDP, ICMP, etc.).

j) O serviço deve ser capaz de detectar anomalias no tráfego, ataques ainda não conhecidos e criar bloqueios em tempo real sem intervenção manual do administrador.

6.4.11. como para Ipv6, incluindo, mas não se restringindo aos seguintes:

6.4.12. O Serviço deve ser capaz de mitigar ataques DDoS na nuvem de forma automatizada, configurando thresholds diferenciados para os níveis de proteção criados que, se atingidos, redirecionem o tráfego para o centro de limpeza da CONTRATADA, para posterior devolução do tráfego limpo à rede da CONTRATANTE.

6.4.13. A CONTRATADA deve realizar a mitigação de ataques e limpeza do tráfego ilegítimo sem prejudicar ou impedir o tráfego legítimo, seja ele originado de uma ou mais fontes.

6.4.14. A CONTRATADA deve atuar na detecção de Falsos-Positivos e promover medidas proativas para que bloqueios indevidos não ocorram e nem impacte no tráfego de negócio da CONTRATANTE, desde que as atividades relacionadas estejam devidamente autorizadas pela CONTRATANTE por e-mail ou mediante atendimento de chamado técnico.

6.5. CARACTERÍSTICAS DA SOLUÇÃO DE SEGURANÇA (NGFW)

6.5.1. CARACTERÍSTICAS GERAIS DA SOLUÇÃO NGFW

i. 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.

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

iii. 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.

iv. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

v. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação.

vi. A gestão do equipamento deve ser compatível através da interface de gestão Web

no mesmo dispositivo de proteção da rede.

vii. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q.

viii. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP.

ix. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding.

x. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM).

xi. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay.

xii. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server.

xiii. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames.

xiv. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas.

xv. Deve suportar NAT dinâmico (Many-to-1).

xvi. Deve suportar NAT dinâmico (Many-to-Many).

xvii. Deve suportar NAT estático (1-to-1).

xviii. Deve suportar NAT estático (Many-to-Many).

xix. Deve suportar NAT estático bidirecional 1-to-1.

xx. Deve suportar Tradução de porta (PAT).

xxi. Deve suportar NAT de Origem.

xxii. Deve suportar NAT de Destino.

xxiii. Deve suportar NAT de Origem e NAT de Destino simultaneamente.

xxiv. Deve poder combinar NAT de origem e NAT de destino na mesma política

xxv. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

xxvi. Deve suportar NAT64 e NAT46.

xxvii. Deve implementar o protocolo ECMP.

xxviii. Deve implementar balanceamento de link por hash do IP de origem.

xxix. Deve implementar balanceamento de link por hash do IP de origem e destino.

xxx. 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.

xxxi. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais.

xxxii. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede.

xxxiii. Enviar log para sistemas de monitoração externos, simultaneamente.

xxxiv. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL.

xxxv. Proteção anti-spoofing.

xxxvi. Implementar otimização do tráfego entre dois equipamentos.

xxxvii. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).

xxxviii. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).

xxxix. Suportar OSPF graceful restart.

xl. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3).

xli. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

xlii. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego.

xliii. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego.

xliv. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

xlv. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente.

xlvi. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3.

xlvii. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster.

xlviii. A configuração em alta disponibilidade deve sincronizar: Sessões.

xlix. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede.

l. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs.

li. A configuração em alta disponibilidade deve sincronizar:Tabelas FIB.

lii. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

liii. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance.

liv. 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.

lv. 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.

lvi. 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).

lvii. Deve apoiar um tecido de segurança para fornecer uma solução de segurança holística abrangendo toda a rede.

lviii. O tecido de segurança deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede.

lix. Deve existir um Serviço de Suporte que oferece aos clientes uma verificação de saúde recorrente com um relatório de auditoria mensal personalizado de seus appliances NGFW.

6.5.2. CONDIÇÕES DO FORNECIMENTO DOS APPIANCES

a) A CONTRATADA deverá comunicar à CONTRATANTE, antecipadamente, a data e o horário da entrega, não sendo aceitos os produtos que estiverem em desacordo com as especificações constantes deste instrumento.

b) A CONTRATADA deverá se responsabilizar por todos os ônus relativos ao fornecimento dos equipamentos inclusive frete, seguro, cargas e descargas desde a origem até sua entrega no local de instalação

6.5.3. MANUAIS E DOCUMENTAÇÃO

a) A CONTRATADA deverá indicar os sites dos fabricantes envolvidos nesta solução que devem obrigatoriamente oferecer download gratuito de todas as atualizações de drivers de dispositivos e firmwares para os equipamentos ofertados bem como dispor dos manuais técnicos com informações detalhadas e atualizadas sobre instalação, configuração, operação e administração dos equipamentos.

6.5.4. TRANSFERÊNCIA DE CONHECIMENTO

a) A CONTRATADA deverá fazer a transferência de conhecimento de no mínimo 40 (quarenta) horas para até 6 (seis) funcionários a ser definidos pela CONTRATANTE. O repasse de conhecimento visa um treinamento básico de startup das soluções e não um treinamento oficial.

b) A transferência de conhecimento será feita nas dependências da CONTRATANTE e não inclui nenhum tipo de material didático ou certificado.

6.5.5. TREINAMENTO OFICIAL

a) Deverão ser ofertadas 3 (três) vagas para treinamento oficial de configuração, administração e utilização de TODOS OS COMPONENTES DE HARDWARE E SOFTWARE desta solução. Todos os materiais didáticos, ou seja, cada um dos 3 (três) participantes deverão receber o seu material didático oficial do fabricante.

b) A CONTRATADA não será responsável pelos valores de logísticas, hospedagem e alimentação. Somente pelo fornecimento dos vouchers para o treinamento oficial, estes citados acima.

c) Os treinamentos deverão ser ministrados por instrutores especialistas nos respectivos componentes da solução e que detenha todas as condições técnicas (teóricas e práticas) necessárias para desempenhar tal função.

d) Na conclusão de cada treinamento, deverão ser entregues a cada um dos 3 (três) participantes um certificado de conclusão do treinamento.

6.5.6. CONSOLE DE GERÊNCIA E MONITORAMENTO

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

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

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

d) O gerenciamento deve permitir/possuir:

1. Criação e administração de políticas de firewall e controle de aplicação.
2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware.
3. Criação e administração de políticas de Filtro de URL.
4. Monitoração de logs.
5. Ferramentas de investigação de logs.
6. Debugging.
7. Captura de pacotes.

e) Acesso concorrente de administradores.

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

g) Deve permitir usar palavras chaves e cores para facilitar identificação de regras.

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

i) Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores.

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

k) Autenticação integrada ao Microsoft Active Directory e servidor Radius.

l) Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados.

m) Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QoS.

n) Criação de regras que fiquem ativas em horário definido.

o) Criação de regras com data de expiração.

p) Backup das configurações e rollback de configuração para a última configuração salva.

q) Suportar Rollback de Sistema Operacional para a última versão local.

r) Habilidade de upgrade via SCP, TFTP e interface de gerenciamento.

s) Validação de regras antes da aplicação.

1. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.

t) Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).

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

u) Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

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

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

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

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

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

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

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

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

dd) Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime.

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

ff) Deve ser possível exportar os logs em CSV.

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

hh) Rotação do log.

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

1. Situação do dispositivo e do cluster.
2. Principais aplicações.
3. Principais aplicações por risco.
4. Administradores autenticados na gerência da plataforma de segurança.
5. Número de sessões simultâneas.
6. Status das interfaces.
7. Uso de CPU

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

1. Resumo gráfico de aplicações utilizadas.
2. Principais aplicações por utilização de largura de banda de entrada e saída.
3. Principais aplicações por taxa de transferência de bytes.
4. Principais hosts por número de ameaças identificadas.
5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego.
6. Deve permitir a criação de relatórios personalizados.

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

ll) Gerar alertas automáticos via:

1. Email.
2. SNMP.
3. Syslog.

6.5.7.CAPACIDADE DO APPLIANCE

a) Hardware Specifications
b) GE RJ45 WAN Interfaces 2
c) GE RJ45 Management/HA Ports 2
d) GE RJ45 Ports 14
e) GE SFP Slots 4
f) USB port 1
g) Console (RJ45) 1
h) Local Storage — 1x 480 GB SSD
i) Included Transceivers 0
j) PS Throughput 2 2.2 Gbps
k) NGFW Throughput 2, 4 1.8 Gbps
l) Threat Protection Throughput 2, 5 1.2 Gbps
m) Firewall Throughput
n) (1518 / 512 / 64 byte UDP packets)
o) 20 / 20 / 9 Gbps
p) Firewall Latency (64 byte UDP packets) 3 µs
q) Firewall Throughput (Packets Per Second) 13.5 Mpps
r) Concurrent Sessions (TCP) 2 Million
s) New Sessions/Second (TCP) 135,000
t) Firewall Policies 10,000
u) IPsec VPN Throughput (512 byte) 1 7.2 Gbps
v) Gateway-to-Gateway IPsec VPN Tunnels 2,000
w) Client-to-Gateway IPsec VPN Tunnels 10,000
x) SSL-VPN Throughput 900 Mbps
y) Concurrent SSL-VPN Users
z) (Recommended Maximum, Tunnel Mode)
aa)500
bb)SSL Inspection Throughput (IPS, avg. HTTPS) 3 820 Mbps
cc) SSL Inspection CPS (IPS, avg. HTTPS) 3 1,000
dd)SSL Inspection Concurrent Session
ee)(IPS, avg. HTTPS) 3
ff) 240,000
gg)Application Control Throughput (HTTP 64K) 2 3.5 Gbps
hh)CAPWAP Throughput (1444 byte, UDP) 1.5 Gbps
ii) Virtual Domains (Default / Maximum) 10 / 10
jj) Maximum Number of FortiSwitches Supported 24
kk) Maximum Number of FortiAPs
ll) (Total / Tunnel Mode)
mm) 128 / 64
nn)Maximum Number of FortiTokens 5,000
oo)Maximum Number of Registered FortiClients 600
pp)High Availability Configurations Active / Active, Active / Passive, Clustering
qq)Height x Width x Length (inches) 1.75 x 17.0 x 11.9
rr) Height x Width x Length (mm) 44.45 x 432 x 301
ss) Weight 11.9 lbs (5.4 kg) 12.12 lbs (5.5 kg)
tt) Form Factor Rack Mount, 1 RU
uu)Power 100–240V AC, 50–60 Hz
vv) Maximum Current 110 V / 3 A, 220 V / 0.42 A

ww) Power Consumption (Average / Maximum) 70.98 / 109.9 W
xx) Heat Dissipation 374.9 BTU/h
yy) Operating Temperature 32–104°F (0–40°C)
zz) Storage Temperature -31–158°F (-35–70°C)
aaa) Humidity 10–90% non-condensing
bbb) Noise Level 31.1 dBA
ccc) Operating Altitude Up to 7,400 ft (2,250 m)
ddd) Compliance FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL,
eee) CB, BSMI
fff) Certifications ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN;
ggg) IPv6

6.5.8. CONTROLE POR POLÍTICA DE FIREWALL

a) Deverá suportar controles por zona de segurança.

b) Controles de políticas por porta e protocolo.

c) Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

d) Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

e) Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis.

f) Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall.

g) Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise).

h) Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF).

i) Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não supere a velocidade de upload.

j) Deve suportar o protocolo padrão da indústria VXLAN.

6.5.9. CONTROLE DE APLICAÇÕES

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

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

c) 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.

d) 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.

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

f) Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária.

g) 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.

h) 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.

i) 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.

j) Identificar o uso de táticas evasivas via comunicações criptografadas.

k) Atualizar a base de assinaturas de aplicações automaticamente.

l) Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos.

m) 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.

n) 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.

o) Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.

p) Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações

desconhecidas e não somente sobre aplicações conhecidas.

q) 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.

r) 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.

s) O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

t) Deve alertar o usuário quando uma aplicação for bloqueada.

u) Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos.

v) Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos.

w) Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo.

x) Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos.

y) 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).

z) Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação.

aa) Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

6.5.10. PREVENÇÃO DE AMEAÇAS

a) 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.

b) Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).

c) 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.

d) Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando

implementado em alta disponibilidade.

e) 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.

f) As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

g) Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.

h) Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.

i) Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

j) Deve permitir o bloqueio de vulnerabilidades.

k) Deve permitir o bloqueio de exploits conhecidos.

l) Deve incluir proteção contra ataques de negação de serviços.

m) Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de padrões de estado de conexões.

n) Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo.

o) Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo.

p) Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise heurística.

q) Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation.

r) Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP.

s) Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados.

t) Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

u) Detectar e bloquear a origem de portscans.

v) Bloquear ataques efetuados por worms conhecidos.

w) Possuir assinaturas especificas para a mitigação de ataques DoS e DDoS.

x) Possuir assinaturas para bloqueio de ataques de buffer overflow.

y) Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.

z) 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.

aa) Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.

bb) Identificar e bloquear comunicação com botnets.

cc) 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.

dd) Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação.

ee) Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.

ff) Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.

gg) Os eventos devem identificar o país de onde partiu a ameaça.

hh) Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

ii) Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.

jj) 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.

kk) O Firewall deve permitir que se analise a implantação de Tecido de Segurança para identificar potenciais vulnerabilidades e destaque as práticas recomendadas que podem ser usadas para melhorar a segurança e o desempenho geral da rede.

ll) Caso o firewall possa ser coordenado por software de segurança do computador do usuário final (laptop, desktop, etc.) deve ter um perfil onde se possa executar a análise de vulnerabilidade nestes equipamentos de usuário e assegurar que estes executem versões compatíveis.

mm) Análise de postura de segurança devem existir para permitir que o software de segurança do endpoint aplique proteção em tempo real, antivírus, filtragem da Web e controle de aplicativos no endpoint.

nn) Fornecer proteção contra ataques de dia zero por meio de estreita integração com os componentes Security Fabric, incluindo NGFW, Sandbox (on-premise e nuvem).

6.5.11. FILTRO DE URL

a) Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

b) Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.

c) 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.

d) Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.

e) Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs.

f) Possuir pelo menos 60 categorias de URLs.

g) Deve possuir a função de exclusão de URLs do bloqueio, por categoria.

h) Permitir a customização de página de bloqueio.

i) 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).

j) Além do Explicit Web Proxy, suportar proxy Web transparente.

6.5.12. IDENTIFICAÇÃO DE USUÁRIOS

a) 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.

b) 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.

c) Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2.

d) 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.

e) Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

f) Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

g) 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).

h) 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.

i) Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

j) Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução.

k) Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

6.5.13. QoS E TRAFFIC SHAPING

a) 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 máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

b) Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem.

c) Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino.

d) Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo.

e) Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus.

f) Suportar a criação de políticas de QoS e Traffic Shaping por porta.

g) O QoS deve possibilitar a definição de tráfego com banda garantida.

h) O QoS deve possibilitar a definição de tráfego com banda máxima.

i) O QoS deve possibilitar a definição de fila de prioridade.

j) Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

k) Suportar marcação de pacotes Diffserv, inclusive por aplicação.

l) Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping.

m) Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

6.5.14. FILTRO DE CONTEÚDO

a) Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc).

b) Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

c) Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

d) 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.

6.5.15. GEOLOCALIZAÇÃO

a) Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado Pais/Países sejam bloqueados.

b) Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

c) Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

6.5.16. 1VPN IPSec

a) Suportar VPN Site-to-Site e Cliente-To-Site.

b) Suportar IPSec VPN.

c) Suportar SSL VPN.

d) A VPN IPSEc deve suportar 3DES.

e) A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.

f) A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

g) A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).

h) A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard).

i) A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.

j) Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

k) Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting.

l) 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.

m) A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

n) 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.

o) Atribuição de DNS nos clientes remotos de VPN.

p) Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

q) Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local.

r) Suportar leitura e verificação de CRL (certificate revocation list).

s) Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

t) Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Antes do usuário autenticar na estação.

u) Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Após autenticação do usuário na estação.

v) Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Sob demanda do usuário.

w) Deverá manter uma conexão segura com o portal durante a sessão.

x) O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior).

7. DOS LOCAIS DE PRESTAÇÃO DO SERVIÇO

Órgão deverá disponibilizar a relação dos endereços e velocidades que deverão ser entregues na solução.

8. DOS PRAZOS DE EXECUÇÃO DOS SERVIÇOS

8.1. ELABORAÇÃO DO PLANO DE IMPLANTAÇÃO

8.1.1. A CONTRATADA deverá apresentar um Plano de Implantação em no máximo 10 (dez) dias corridos a partir da assinatura do Contrato.

8.1.2. A execução do Plano de Implantação somente poderá ser iniciada após a sua aprovação pela CONTRATANTE.

8.1.3. O detalhamento do Plano de Implantação deverá conter no mínimo:

a) Cronograma com macro atividades a serem desenvolvidas para a implantação de todos os serviços previstos neste Termo de Referência. O cronograma deverá conter as seguintes informações:

- Identificação dos responsáveis das atividades.
- Duração das atividades.

- Sequenciamento das atividades.

b) Projeto com topologias (física e lógica) da rede, elementos envolvidos, localização dos POPs, faixas de endereçamento IP, detalhamento da gerência, bem como a arquitetura do serviço, incluindo a estratégia de roteamento.

8.2. DA INSTALAÇÃO DOS SERVIÇOS

8.2.1. A CONTRATADA terá até trinta (30) dias corridos após a assinatura do contrato para instalar os serviços especificados no Edital e Termo de Referência.

8.2.2. A instalação do circuito e CPE somente será considerada concluída após a aprovação, pelo Gestor do Contrato, que ocorrerá em até 5 (cinco) dias corridos após notificação da CONTRATADA.

8.2.3. Todos os equipamentos deverão suportar alimentação com tensão de 110/220 Volts (corrente alternada) bifásica com frequência de 60 Hz.

8.3. DO GERENCIAMENTO DA IMPLANTAÇÃO

8.3.1. Disponibilizar e alocar 1 (um) profissional que será responsável pelo gerenciamento das atividades do projeto de implantação, por parte da CONTRATADA.

8.3.2. Obter informações e esclarecimentos necessários para que possa elaborar o Plano de Implantação do Serviço. Serão abordados e discutidos os seguintes pontos:

a) Instalação dos circuitos.

b) Datas e horários de restrição para implantação.

c) Requisitos de infraestrutura necessários para a instalação dos equipamentos.

d) Requisitos para a elaboração e entrega do Plano de Implantação do Serviço.

e) Serviços que deverão ser configurados na implantação.

f) Demais assuntos de interesse correlatos à implantação dos serviços.

8.3.1. Apresentar ao Gestor do Contrato do CONTRANTE o(s) profissional(is) que atuará(ão) como preposto(s) da empresa para assuntos relativos à execução contratual, e informar ao CONTRANTE o nome completo e o CPF deste(s) preposto(s).

9. CENTRAL DE ATENDIMENTO E SUPORTE TÉCNICO

9.1. A fim de manter os serviços em funcionamento adequado aos parâmetros contratuais, a CONTRATADA deverá:

9.1.1. Possuir um Centro de Operações de Rede (Network Operations Center – NOC) disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável por monitorar o funcionamento dos serviços e realizar as ações corretivas necessárias para restabelecer a normalidade dos serviços.

9.1.2. Possuir uma equipe especializada (SOC - Security Operation Center), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável pelo monitoramento,

detecção e mitigação de ataques, realizando as ações corretivas necessárias para garantir o bom funcionamento dos serviços.

9.1.3. A CONTATADA deverá disponibilizar à CONTRATANTE uma Central de Atendimento Técnico, acessível via chamada telefônica gratuita (0800), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável por prestar suporte técnico, receber chamados de serviços e prestar informações acerca do andamento destes.

9.1.4. O limite de atuação da CONTRATADA para fins de manutenção, reparo e configuração será a porta LAN de seus roteadores ou switches, de forma a garantir os níveis de serviço contratados.

9.1.5. Enviar à CONTRATANTE, por e-mail, notificações de abertura, andamento e fechamento de chamados, realização de manutenção preventiva ou corretiva e fatos relevantes para a prestação e utilização dos serviços.

9.1.6. Enviar à CONTRATANTE, por e-mail, uma lista de recorrência ("escalation list") contendo os nomes, números de telefone e endereços de e-mail das pessoas que devem ser acionadas em caso de problemas no atendimento técnico. A lista de recorrência deverá ser mantida atualizada e sua versão mais recente deverá ser enviada à CONTRATANTE sempre que houver alteração.

9.1.7. A CONTRATADA deverá iniciar o atendimento no prazo máximo de 1 (uma) hora, contada a partir da data e hora do chamado.

9.1.8. Todo acesso às instalações da CONTRATANTE por pessoal técnico da CONTRATADA, ou de seu preposto, deverá ser previamente agendado.

9.1.9. Manutenções e/ou intervenções programadas nos serviços, quando necessárias, mesmo no caso daquelas que não impliquem inoperância dos serviços contratados ou alteração nas suas características, que necessitem a presença do técnico da CONTRATADA, deverão ser autorizadas pela CONTRATANTE.

9.1.10. Qualquer manutenção e/ou intervenção de caráter emergencial para solução de falhas, inoperâncias e/ou indisponibilidades, verificadas na rede, deverá ser agendada e acordada previamente com a CONTRATANTE.

10. PORTAL DE GERENCIAMENTO E ACOMPANHAMENTO DOS SERVIÇOS

10.1. A CONTRATADA deverá disponibilizar um Portal WEB de gerência, possibilitando a visualização online dos serviços prestados, como também realizar o registro e acompanhamento dos chamados.

10.1.1. Consulta e visualização online: O Portal deverá apresentar informações relativas aos ativos de rede utilizados com as seguintes funcionalidades:

a) Alertas em caso de falhas e anormalidade dos circuitos.

b) Topologia da rede, incluindo roteadores e circuitos, com a visualização do status de todos os elementos.

c) Visualização da utilização de banda dos circuitos, de forma diária, semanal e mensal, com a opção de consulta de dados históricos de até 3 (três) meses.

d) Visualização do consumo de CPU e memória dos roteadores.

e) Indicação da taxa de perda de pacotes, latência e disponibilidade nos circuitos.

f) Inventario dos roteadores contendo a configuração física de cada equipamento (interfaces, memoria, cpu, etc). modelo e fabricante. endereços IPs e máscaras.

10.1.2. Registro e acompanhamento dos chamados:

Permitir o acompanhamento dos registros de problemas e das ações executadas para a recuperação dos serviços, relativos à pelo menos aos últimos 90 (noventa) dias, incluindo as seguintes informações:

a) Identificação do registro (número de chamado).
b) Data e hora de abertura do chamado (registro).
c) Descrição do problema.
d) Identificação do reclamante (nome e telefone).
e) Data e hora de conclusão do atendimento (fechamento do chamado).
f) Ações realizadas para a solução do problema.

11. GERENCIAMENTO PROATIVO

11.1. A CONTRATADA deverá prover o gerenciamento proativo, com funcionamento 24 horas por dia, 7 (sete) dias na semana, incluindo sábados, domingos e feriados. Entende-se por gerenciamento proativo a capacidade da CONTRATADA de detectar falhas ocorridas nos circuitos (serviços e equipamentos) de forma autônoma e independentemente de notificação por parte da CONTRATANTE. Da mesma forma autônoma a CONTRATADA deve dar início aos procedimentos de correção de falhas e em seguida informar a CONTRATANTE sobre o evento. A CONTRATADA deverá notificar a CONTRATANTE através de telefones e e-mails definidos pela CONTRATANTE no prazo máximo de 25 minutos após a identificação do incidente.

11.2. Gerência exclusiva de relacionamento para acompanhamento, apresentação da evolução e gestão da rede, que fará mensalmente o agendamento e apresentação dos relatórios, através de videoconferência ou por e-mail.

11.3. Atividades realizadas pela equipe responsável pelo gerenciamento proativo:

a) Gerenciamento individualizado da rede.
b) Relatórios mensais sobre a performance da rede.
c) Relatório Gráfico de indisponibilidade.
d) Relatório de tráfego de qualidade.

e) Relatório de Consumo de Banda.

f) Relatório de Eventos ocorridos.

g) Relatório de Disponibilidade dos serviços.

h) Gerenciamento de desempenho proativo.

12. DISPONIBILIDADE

12.1. Índice de Disponibilidade:

12.1.1. Os circuitos de comunicação deverão estar disponíveis 24 horas por dia, todos os dias do ano.

12.1.2. A CONTRATADA deverá garantir disponibilidade mensal de no mínimo, 99,5% para cada circuito fornecido à CONTRATANTE, calculada da seguinte forma:

DMA = [(43200 - TTICM) / 43200] x 100

Onde:

TTICM: Tempo Total de Interrupção do Circuito (em minutos) no Mês.

DMA(%): Disponibilidade Mensal Atingida

12.1.3. Para efeito de cálculo de TTICM, será considerado o período em minutos entre o primeiro minuto do primeiro dia e o último minuto do último dia do calendário do mês a que se refere a fatura.

12.1.4. O serviço será considerado indisponível quando não for possível a conexão entre o equipamento da CONTRATANTE e o da CONTRATADA, a partir do registro do chamado técnico na Central de Atendimento da CONTRATADA, sendo considerado disponível após o fechamento do chamado técnico, com a devida anuência da CONTRATANTE, na Central de atendimento da CONTRATADA.

12.1.5. Entende-se como início do atendimento a primeira mensagem trocada pela CONTRATANTE com a CONTRATADA informando a ocorrência ou início da ligação efetuada a central de atendimento da CONTRATADA independentemente do atendimento do operador.

12.1.6. O prazo máximo de recuperação dos circuitos será 2 (duas) horas, todos os dias do mês, inclusive sábados, domingos e feriados.

12.1.7. As indisponibilidades informadas pela gerência e supervisão da CONTRATADA, bem como os registros na Central de Atendimento da CONTRATADA serão validadas pelos sistemas de gerência e supervisão da CONTRATANTE.

12.1.8. No caso de interrupção programada por necessidade da CONTRATANTE, a mesma não afetará o índice de disponibilidade da CONTRATADA.

12.1.9. As interrupções programadas solicitadas pela CONTRATANTE serão previamente combinadas com a CONTRATADA.

12.2. Desconto por interrupção:

12.2.1. Para cada interrupção do circuito que for comprovadamente de responsabilidade da CONTRATADA, será calculado um desconto referente ao tempo de interrupção desse circuito, cujo valor apurado será ressarcido à CONTRANTANTE na Nota Fiscal/Fatura dos serviços com vencimento no mês seguinte ao da apuração.

12.2.2. O valor do desconto será obtido a partir do seguinte cálculo:

VD = (VC / 43200) x n

Onde:

VD = Valor do Desconto

VC = Valor mensal pago pelo circuito ativo

n = Quantidade de minutos em que o serviço ficou interrompido.

13. NÍVEIS MÍNIMOS DE SERVIÇO

A CONTRATADA deverá fornecer o serviço com os seguintes níveis mínimos de disponibilidade, latência e taxa máxima de erro, os quais são utilizados para mensurar o desempenho e a qualidade dos circuitos:

Métrica	Nível Mínimo de Serviço
Disponibilidade do circuito IP	>= 99,5%
Latência	<= 1ms
Perda de pacotes	<=2%

14. DAS OBRIGAÇÕES

14.1. OBRIGAÇÕES DA CONTRATANTE

a) Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta.

b) Comunicar oficialmente à CONTRATADA sobre quaisquer falhas verificadas na fiscalização do cumprimento dos serviços prestados.

c) Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção.

d) Efetuar o pagamento devido pela execução do(s) serviço(s) dentro do prazo estipulado, desde que cumpridas todas as formalidades e exigências contratuais.

e) Acompanhar as visitas, inspeções, reuniões solicitadas pela CONTRATADA.

f)Prestar, por meio do Gestor do Contrato, as informações e os esclarecimentos pertinentes ao(s) serviço(s) contratado(s) que venham a ser solicitados pela

CONTRATADA.

g) Registrar os incidentes e problemas ocorridos durante a execução do Contrato.

h) Proporcionar os recursos necessários, técnicos e logísticos, dentro dos locais de instalação dos equipamentos para que a CONTRATADA possa executar os serviços conforme as especificações estabelecidas no Termo de Referência.

i) Permitir acesso dos empregados da CONTRATADA, desde que devidamente credenciados, às suas dependências para a realização dos serviços.

j) Aplicar as sanções previstas, assegurando à CONTRATADA o contraditório e à ampla defesa.

14.2. OBRIGAÇÕES DA CONTRATADA

a) Prestar os esclarecimentos que forem solicitados pelo CONTRATANTE, bem como dar ciência ao mesmo, imediatamente e por escrito, de qualquer anormalidade que verificar.

b) Comunicar imediatamente ao CONTRATANTE qualquer alteração ocorrida na conta bancária, endereço e outras informações necessárias para recebimento de correspondências e pagamento.

c) Responsabilizar-se pelo exato cumprimento de todas as obrigações e exigências decorrentes da legislação trabalhista e previdenciária, ficando claro inexistir entre seus empregados e o CONTRATANTE vínculo empregatício ou de qualquer outra natureza, razão pela qual correrão por conta exclusiva da CONTRATADA todos os ônus decorrentes de rescisões de contratos de trabalho e atos de subordinação de seu pessoal.

d) Arcar com todos os encargos sociais trabalhistas, tributos de qualquer espécie que venham a ser devidos em decorrência da execução do serviço contratado, bem como custos relativos ao deslocamento e estada de seus profissionais, caso exista.

e) Manter, durante a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação exigidas em razão da natureza das atividades prestadas e do certame licitatório.

f) Fazer diagnóstico das falhas no serviço relatadas pelo CONTRATANTE dentro do prazo estipulado.

g) Providenciar a recuperação de falhas na prestação do serviço, comunicadas pelo CONTRATANTE mantendo-o informado sobre as ações efetivadas até a completa normalização da prestação do serviço.

h) Respeitar o sistema de segurança do CONTRATANTE e fornecer todas as informações solicitadas por ele

i) Credenciar junto ao CONTRATANTE um representante, para prestar esclarecimentos e atender às reclamações que porventura surgirem durante a execução do contrato.

j) O CONTRATANTE não aceitará a transferência de responsabilidade da CONTRATADA

para terceiros.

k) Prestar o serviço contratado conforme especificações, prazos e demais condições estabelecidas no Termo de Referência.

l) Utilizar melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações contidas neste Contrato e no Termo de Referência.

m) Reportar formal e imediatamente ao Gestor do Contrato quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução do(s) serviço(s)

n) Atender e prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da área de tecnologia da Informação do CONTRATANTE, referentes a qualquer problema detectado ou ao andamento de atividades previstas.

o) Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas neste instrumento, caso os prazos, indicadores e condições não sejam cumpridos.

p) Manter seus profissionais nas dependências do CONTRATANTE adequadamente trajados e identificados com uso permanente de crachá, com foto e nome visível.

q) Manter-se, durante toda a execução do contrato, em conformidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

15. DA VIGÊNCIA DO CONTRATO

15.1. O contrato terá período de vigência de 12 (doze) meses. Podendo ser prorrogado por meio de termo aditivo.

16. DISPOSIÇOES FINAIS

16.1. Não serão aceitas propostas que apresentem preço global ou unitário simbólicos, irrisórios ou de valor zerado, incompatíveis com os preços pelo mercado.

17. DA VISITA TÉCNICA

17.1. É facultado aos interessados a realização de visita técnica no Hospital Municipal de Aparecida de Goiânia, localizado na Avenida V5 e V7, – Cidade Vera Cruz – Aparecida de Goiânia/GO, para levantamento do perfil e especificações dos serviços.

18. DA CONTRATAÇÃO

18.1. O IBGH não tem a obrigação de contratar o serviço publicado, e podendo optar também, na contratação parcial destes.

18.2. As propostas terão validade de 90 (noventa) dias, após a apresentação da mesma.

Aparecida de Goiânia/Go, 11 de outubro de 2019.

Jefferson Tadeu de Oliveira
Gerente de TI
Hospital Municipal de Aparecida de Goiânia - HMAP

Jefferson Tadeu de Oliveira

Gerencia de Tecnologia da Informação

MINUTA CONTRATUAL

CONTRATO XX/XX – HMAP

CONTRATO DE NA PRESTAÇÃO DE SERVIÇOS DE INTERNET

QUADRO 01 – DOS DADOS DAS PARTES	
CONTRATANTE:	
INSTITUTO BRASILEIRO DE GESTÃO HOSPITALAR – IBGH	**CNPJ:** 18.972.378/0009-70
	ENDEREÇO: Av. V-5, S/N, Qd. A, Área Lt.001-E SALA 01, Cidade Vera Cruz, Aparecida de Goiânia – Goiás, CEP: 74.936-600
	NESTE ATO REPRESENTADO POR SEU SUPERINTENDENTE: Estêvão Costa Daltro
	CPF: 467.255.551-87
CONTRATADA	
XXX	**CNPJ:** XXX
	ENDEREÇO: XXX
	REPRESENTANTE LEGAL: XXX
	CPF: XXX
	RG: XXX

QUADRO 02 – DA UNIDADE DE SAÚDE, VIGÊNCIA CONTRATUAL E OBJETO	
UNIDADE DE SAÚDE	
HOSPITAL MUNICIPAL DE APARECIDA DE GOIÂNIA HMAP	**MUN./UF** Aparecida de Goiânia – GO.
	CONTRATO DE GESTÃO: 1095/2018 -SEL
VIGÊNCIA CONTRATUAL: 12 (doze) meses.	
INÍCIO: A partir da emissão da **ordem de serviço**	
POSSIBILIDADE DE PRORROGAÇÃO: Podendo ser renovado anualmente (ou na data de vencimento) formalizado por meio de aditivo em razão da necessidade ou conveniência de continuação da prestação do serviço/fornecimento dos produtos devidamente justificada, sendo limitado a vigência do Contrato de Gestão em referência.	
PRAZO VINCULADO AO CONTRATO DE GESTÃO: Em caso de rescisão, por qualquer motivo, do Contrato de Gestão ao qual esta contratação está vinculada, o contrato firmado entre a CONTRATANTE e a CONTRATADA será rescindido, independente de prévio aviso ou notificação.	
ESPECIFICAÇÃO DO OBJETO E NATUREZA DO CONTRATO	
OBJETO: CONTRATO DE NA PRESTAÇÃO DE SERVIÇOS DE INTERNET	
NATUREZA: Prestação de serviços	

QUADRO 03 – DOS SERVIÇOS E ATUAÇÃO TÉCNICA

SERVIÇOS A SEREM EXECUTADOS

1. ESPECIFICAÇÕES TÉCNICAS DO OBJETO:

1.1 REQUISITOS GERAIS

•Contratação de empresa especializada para o fornecimento de acesso à Rede Mundial de Internet com 100% de garantia de banda downstream e upstream, full-duplex, com conectividade em protocolos IPv4 e IPv6.

- Toda a infraestrutura de rede, acesso e CPE da CONTRATADA deverão ser dimensionadas e preparadas para suportar a totalidade do serviço.
- A CONTRATADA deverá reservar os canais de comunicação e as portas de acesso à sua infraestrutura para uso exclusivo da CONTRATANTE; não sendo admitido o compartilhamento desses recursos com outro de seus clientes ou usuários
- acesso referido no item anterior deverá ser provido por meio de backbone próprio da prestadora de serviço.
- Os equipamentos da CONTRATADA utilizados em toda a solução deverão ser novos e compatíveis com ambientes corporativos ou institucionais modernos.
- A CONTRATADA obriga-se e se responsabiliza a prestar o serviço objeto da licitação, por meio de mão de obra especializada e devidamente qualificada, necessário à completa e perfeita execução dos serviços, em conformidade com as especificações do Termo de Referência.
- Será de responsabilidade da CONTRATANTE o fornecimento de energia elétrica para alimentação dos equipamentos nas dependências das unidades, o aterramento da rede elétrica e a climatização das dependências.

2. CARACTERÍSTICAS DO LINK INTERNET

- Fornecer e instalar link de Internet na taxa de 200Mbps dedicado.
- CONTRATADA deverá disponibilizar 04 endereços IPV4 e 04 endereços IPv6 fixos e válidos para provimento da solução de Internet.
- A conexão entre o CPE da CONTRATADA e o equipamento da CONTRATANTE deverá ser realizada através de interface Gigabit Ethernet 1000BASE-TX.
- A CONTRATADA poderá utilizar acessos de terceiros como última milha, sendo de inteira responsabilidade da CONTRATADA o cumprimento dos SLAs especificados 99.5%.
- A velocidade do link do serviço entregue à CONTRATANTE deverá ser correspondente a 100% da banda contratada.

•acesso físico (conexão entre o ponto de presença da CONTRATADA e os equipamentos de comunicação de dados da CONTRATADA instalados nas dependências da CONTRATANTE) deverá ser realizado exclusivamente por meio de fibra óptica, sendo vedada a utilização de qualquer outra tecnologia de acesso.

- O serviço de Internet deverá ser entregue em rede roteada, utilizando protocolos de camada 3, com SLA 99,5% de disponibilidade e MTTR de vinte quatro (24) horas
- Disponibilizar serviço de Domain Name Resolution (DNS) da CONTRATADA, capaz de resolver direta e reversamente endereços de Internet, para registro no servidor DNS primário.
- Ser monitorado em regime 24x7 por centro de monitoração da CONTRATADA, sendo responsável pela administração e gerência de equipamentos e links de comunicação de dados, manutenção dos níveis mínimos de serviços exigidos e prevenção e recuperação de falhas de serviço.
- Disponibilizar informações sobre os serviços de acesso à Internet por meio de um portal de monitoramento, com acesso restrito, utilizando protocolo seguro (HTTPS), contendo estatísticas de desempenho e de disponibilidade do acesso.
- Possibilitar que a equipe técnica da CONTRATANTE realize consultas no portal de monitoramento, bem como visualize relatórios das informações de desempenho dos serviços contratados
- A CONTRATADA não poderá:

a) Implementar nenhum tipo de filtro de pacotes que possa incidir sobre o tráfego originado ou destinado à CONTRATANTE, a menos que tenha expressa concordância com esta.

b) Implementar nenhum tipo de cache transparente, a menos que tenha expressa concordância da CONTRATANTE.

3. CARACTERÍSTICAS DO ROTEADOR

• O roteador a ser instalado no ambiente da CONTRATANTE deverá ter no mínimo as seguintes características técnicas:

a) O equipamento e seus módulos e softwares não deverão constar em nenhuma lista do fabricante com as situações de "End-of-Sale", "End-of-Order", "End-of-Life" ou "End-of-Support".

b) Deve possuir no mínimo quatro (04) interfaces Gigabit Ethernet padrão 1000BASE-TX.

- Possuir protocolo SNMP habilitado com acesso de leitura.
- Deve implementar os protocolos de roteamento RIP, OSPFv2, OSPFv3 e BGP-4.
- Deve possuir suporte nativo ao protocolo IPv6.
- Deve possuir suporte ao protocolo Netflow v9 ou superior.
- Deve possuir suporte ao protocolo 802.1q.
- Deve possuir suporte aos protocolos Telnet e SSHv2.
- Deve possuir gerenciamento local através de uma porta console, sendo que todos os cabos e adaptadores necessários para o gerenciamento através da porta console deverão ser fornecidos pela CONTRATADA de forma a propiciar o gerenciamento do roteador a partir de uma porta USB.
- Deverá ser disponibilizado para a CONTRATANTE com o último release de software estável disponibilizado pelo fabricante, capaz de atender a todos os requisitos acima, incluindo o suporte à atualização do referido software durante o período de vigência do contrato.
- Deve ser montável em rack padrão EIA-310 com largura padrão 19" ocupando no máximo 1U de altura.

4. CARACTERÍSTICAS DO SERVIÇO Anti DDoS

- A CONTRATADA deverá prover, no âmbito do serviço de segurança do link de Internet, uma solução para identificação, tratamento e mitigação transparente de ataques volumétricos do tipo negação de serviço distribuído (DDoS – Distributed Denial of Service).
- A CONTRATADA deve possuir infraestrutura de mitigação própria com capacidade para conter ataques de grande volume, sendo eles de origem nacional ou internacional. Deverá possuir pelo menos 2 (dois) centros de limpeza, cada um com capacidade de mitigação de 40 Gbps (quarenta gigabits por segundo).
- A CONTRATADA deverá disponibilizar em seu backbone, proteção contra ataques volumétricos de negação de serviço, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DDoS (Distributed Denial of Service).
- A CONTRATADA deverá prover o serviço de mitigação sem limitação de tempo de duração do ataque e com quantidade ilimitada de eventos de ataque ao longo da vigência contratual.

- O ataque deve ser mitigado separando o tráfego legítimo do tráfego malicioso, de modo que os serviços de Internet providos pelo cliente continuem disponíveis.
- A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos.

• Em casos de ataques não detectados pela solução, quando identificados pela CONTRATANTE, deverão ser mitigados imediatamente pelas CONTRATADA após a abertura de chamado através da Central de Atendimento sempre como um chamado com Prioridade Máxima, e deverá realizá-la, sem nenhum ônus ao CONTRATANTE.

• O serviço deve prover suporte à mitigação automática de ataques, utilizando múltiplas técnicas incluindo, mas não se restringindo a: White Lists, Black Lists, limitação de taxa de tráfego, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP, NTP e DNS, bloqueio por localização geográfica de endereços IP.

• A CONTRATADA deve realizar a detecção de ataques utilizando-se dos recursos mais atuais para detecção de ataques de negação de serviço, tais como análise estatística de tráfego, padrões predefinidos para bloqueios de ataques, correlacionamento com ataques que estejam ocorrendo simultaneamente em outras partes do mundo e atualização para detecção de ataques de negação de serviço desconhecidos.

• O serviço deve prover também análise de tráfego baseado em reputação de endereços IP, possuindo base de informações própria, que pode ser gerada durante a filtragem de ataques e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.

- O serviço deve prover mecanismos capazes de detectar e migar todos e quaisquer ataques de DDoS que façam o uso não autorizado de recursos de rede, tanto para Ipv4 Ataques de inundação (Bandwidth Flood), Floods de UDP, TCP e ICMP.
- Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets.
- Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP.
- Ataques provenientes de Botnets, Worms e que utilizam falsificação de endereços IP origem (IP Spoofing).
- Ataques à camada de aplicação, incluindo protocolos HTTP, DNS, NTP, dentre outros.

- O serviço deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pela CONTRATADA.
- O serviço deve permitir a configuração de níveis diferenciados de proteção por grupo de hosts ou subnets.
- O serviço deve ser capaz de bloquear tráfego baseado em assinaturas em até 15 minutos.
- O serviço deve ser capaz de analisar e aprender o comportamento do tráfego para criar automaticamente parâmetros de bloqueio (Limite de conexão HTTP, TCP, UDP, ICMP, etc.).
- O serviço deve ser capaz de detectar anomalias no tráfego, ataques ainda não conhecidos e criar bloqueios em tempo real sem intervenção manual do administrador.

• como para Ipv6, incluindo, mas não se restringindo aos seguintes:

• O Serviço deve ser capaz de mitigar ataques DDoS na nuvem de forma automatizada, configurando thresholds diferenciados para os níveis de proteção criados que, se atingidos, redirecionem o tráfego para o centro de limpeza da CONTRATADA, para posterior devolução do tráfego limpo à rede da CONTRATANTE.

• A CONTRATADA deve realizar a mitigação de ataques e limpeza do tráfego ilegítimo sem prejudicar ou impedir o tráfego legítimo, seja ele originado de uma ou mais fontes.

• A CONTRATADA deve atuar na detecção de Falsos-Positivos e promover medidas proativas para que bloqueios indevidos não ocorram e nem impacte no tráfego de negócio da CONTRATANTE, desde que as atividades relacionadas estejam devidamente autorizadas pela CONTRATANTE por e-mail ou mediante atendimento de chamado técnico.

5. CARACTERÍSTICAS DA SOLUÇÃO DE SEGURANÇA (NGFW)

5.1 CARACTERÍSTICAS GERAIS DA SOLUÇÃO NGFW

- 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.
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
- 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.
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada

- Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP.
- Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding.
- Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM).
- Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay.
- Os dispositivos de proteção de rede devem possuir suporte a DHCP Server.
- Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames.
- Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas.
- Deve suportar NAT dinâmico (Many-to-1).
- Deve suportar NAT dinâmico (Many-to-Many).
- Deve suportar NAT estático (1-to-1).
- Deve suportar NAT estático (Many-to-Many).
- Deve suportar NAT estático bidirecional 1-to-1.
- Deve suportar Tradução de porta (PAT).
- Deve suportar NAT de Origem.
- Deve suportar NAT de Destino.
- Deve suportar NAT de Origem e NAT de Destino simultaneamente.
- Deve poder combinar NAT de origem e NAT de destino na mesma política
- Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
- Deve suportar NAT64 e NAT46.
- Deve implementar o protocolo ECMP.
- Deve implementar balanceamento de link por hash do IP de origem.
- Deve implementar balanceamento de link por hash do IP de origem e destino.
- 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.
- Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais.

- Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede.
- Enviar log para sistemas de monitoração externos, simultaneamente.
- Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL.
- Proteção anti-spoofing.
- Implementar otimização do tráfego entre dois equipamentos.
- Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).
- Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).
- Suportar OSPF graceful restart.
- Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3).
- Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.
- Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego.
- Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego.
- Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente.
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster.
- A configuração em alta disponibilidade deve sincronizar: Sessões.
- A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede.
- A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs.
- A configuração em alta disponibilidade deve sincronizar:Tabelas FIB.
- O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
- Deve possuir suporte a criação de sistemas virtuais no mesmo appliance.
- 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.

- 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.
- 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).
- Deve apoiar um tecido de segurança para fornecer uma solução de segurança holística abrangendo toda a rede.
- O tecido de segurança deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede.
- Deve existir um Serviço de Suporte que oferece aos clientes uma verificação de saúde recorrente com um relatório de auditoria mensal personalizado de seus appliances NGFW.

5.2 CONDIÇÕES DO FORNECIMENTO DOS APPIANCES

a) A CONTRATADA deverá comunicar à CONTRATANTE, antecipadamente, a data e o horário da entrega, não sendo aceitos os produtos que estiverem em desacordo com as especificações constantes deste instrumento.

b) A CONTRATADA deverá se responsabilizar por todos os ônus relativos ao fornecimento dos equipamentos inclusive frete, seguro, cargas e descargas desde a origem até sua entrega no local de instalação

5.3 MANUAIS E DOCUMENTAÇÃO

a) A CONTRATADA deverá indicar os sites dos fabricantes envolvidos nesta solução que devem obrigatoriamente oferecer download gratuito de todas as atualizações de drivers de dispositivos e firmwares para os equipamentos ofertados bem como dispor dos manuais técnicos com informações detalhadas e atualizadas sobre instalação, configuração, operação e administração dos equipamentos.

5.4 TRANSFERÊNCIA DE CONHECIMENTO

a) A CONTRATADA deverá fazer a transferência de conhecimento de no mínimo 40 (quarenta) horas para até 6 (seis) funcionários a ser definidos pela CONTRATANTE. O repasse de conhecimento visa um treinamento básico de startup das soluções e não um treinamento oficial.

A transferência de conhecimento será feita nas dependências da CONTRATANTE e não inclui nenhum tipo de material didático ou certificado.

5.5 TREINAMENTO OFICIAL

- Deverão ser ofertadas 3 (três) vagas para treinamento oficial de configuração, administração e utilização de TODOS OS COMPONENTES DE HARDWARE E SOFTWARE desta solução. Todos os materiais didáticos, ou seja, cada um dos 3 (três) participantes deverão receber o seu material didático oficial do fabricante.
- A CONTRATADA não será responsável pelos valores de logísticas, hospedagem e alimentação. Somente pelo fornecimento dos vouchers para o treinamento oficial, estes citados acima.
- Os treinamentos deverão ser ministrados por instrutores especialistas nos respectivos componentes da solução e que detenha todas as condições técnicas (teóricas e práticas) necessárias para desempenhar tal função.
- Na conclusão de cada treinamento, deverão ser entregues a cada um dos 3 (três) participantes um certificado de conclusão do treinamento.

5.6 CONSOLE DE GERÊNCIA E MONITORAMENTO

- Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento.
- O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.
- Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux.
- O gerenciamento deve permitir/possuir:
- . Criação e administração de políticas de firewall e controle de aplicação.
- . Criação e administração de políticas de IPS, Antivírus e Anti-Spyware.
- . Criação e administração de políticas de Filtro de URL.
- . Monitoração de logs.
- . Ferramentas de investigação de logs.
- . Debugging.
- . Captura de pacotes.
- Acesso concorrente de administradores.
- Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

- Criação de regras que fiquem ativas em horário definido.
- Criação de regras com data de expiração.
- Backup das configurações e rollback de configuração para a última configuração salva.
- Suportar Rollback de Sistema Operacional para a última versão local.
- Habilidade de upgrade via SCP, TFTP e interface de gerenciamento.
- Validação de regras antes da aplicação.
  1. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
- Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).
  1. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).
- Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.
- Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)
- Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.
- Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado.
- Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição.
- Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes.
- O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança.
- Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc.
- Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução.

- Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime.
- Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso.
- Deve ser possível exportar os logs em CSV.
- Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.
- Rotação do log.
- Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
  1. Situação do dispositivo e do cluster.
  2. Principais aplicações.
  3. Principais aplicações por risco.
  4. Administradores autenticados na gerência da plataforma de segurança.
  5. Número de sessões simultâneas.
  6. Status das interfaces.
  7. Uso de CPU
- Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
  1. Resumo gráfico de aplicações utilizadas.
  2. Principais aplicações por utilização de largura de banda de entrada e saída.
  3. Principais aplicações por taxa de transferência de bytes.
  4. Principais hosts por número de ameaças identificadas.
  5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego.
  6. Deve permitir a criação de relatórios personalizados.
- Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos. serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa.
- Gerar alertas automáticos via:
  1. Email.
  2. SNMP.
  3. Syslog.

5.7 CAPACIDADE DO APPLIANCE

- Hardware Specifications
- GE RJ45 WAN Interfaces 2
- GE RJ45 Management/HA Ports 2
- GE RJ45 Ports 14
- GE SFP Slots 4
- USB port 1
- Console (RJ45) 1
- Local Storage — 1x 480 GB SSD
- Included Transceivers 0
- PS Throughput 2 2.2 Gbps
- NGFW Throughput 2, 4 1.8 Gbps
- Threat Protection Throughput 2, 5 1.2 Gbps
- Firewall Throughput
- (1518 / 512 / 64 byte UDP packets)
- 20 / 20 / 9 Gbps
- Firewall Latency (64 byte UDP packets) 3 µs
- Firewall Throughput (Packets Per Second) 13.5 Mpps
- Concurrent Sessions (TCP) 2 Million
- New Sessions/Second (TCP) 135,000
- Firewall Policies 10,000
- IPsec VPN Throughput (512 byte) 1 7.2 Gbps
- Gateway-to-Gateway IPsec VPN Tunnels 2,000
- Client-to-Gateway IPsec VPN Tunnels 10,000
- SSL-VPN Throughput 900 Mbps
- Concurrent SSL-VPN Users
- (Recommended Maximum, Tunnel Mode)
- 500
- SSL Inspection Throughput (IPS, avg. HTTPS) 3 820 Mbps
- SSL Inspection CPS (IPS, avg. HTTPS) 3 1,000
- SSL Inspection Concurrent Session
- (IPS, avg. HTTPS) 3
- 240,000
- Application Control Throughput (HTTP 64K) 2 3.5 Gbps
- CAPWAP Throughput (1444 byte, UDP) 1.5 Gbps
- Virtual Domains (Default / Maximum) 10 / 10
- Maximum Number of FortiSwitches Supported 24
- Maximum Number of FortiAPs
- (Total / Tunnel Mode)
- 128 / 64
- Maximum Number of FortiTokens 5,000
- Maximum Number of Registered FortiClients 600
- High Availability Configurations Active / Active, Active / Passive, Clustering

- Height x Width x Length (inches) 1.75 x 17.0 x 11.9
- Height x Width x Length (mm) 44.45 x 432 x 301
- Weight 11.9 lbs (5.4 kg) 12.12 lbs (5.5 kg)
- Form Factor Rack Mount, 1 RU
- Power 100–240V AC, 50–60 Hz
- Maximum Current 110 V / 3 A, 220 V / 0.42 A
- Power Consumption (Average / Maximum) 70.98 / 109.9 W
- Heat Dissipation 374.9 BTU/h
- Operating Temperature 32–104°F (0–40°C)
- Storage Temperature -31–158°F (-35–70°C)
- Humidity 10–90% non-condensing
- Noise Level 31.1 dBA
- Operating Altitude Up to 7,400 ft (2,250 m)
- Compliance FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL,
- CB, BSMI
- Certifications ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN;
- IPv6

5.8 CONTROLE POR POLÍTICA DE FIREWALL

- Deverá suportar controles por zona de segurança.
- Controles de políticas por porta e protocolo.
- Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
- Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
- Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis.
- Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall.
- Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise).
- Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF).
- Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não supere a velocidade de upload.
- Deve suportar o protocolo padrão da indústria VXLAN.

5.9 CONTROLE DE APLICAÇÕES

- Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.
- Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
- 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.
- 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.
- Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.
- Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária.
- 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.
- 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.
- 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.
- Identificar o uso de táticas evasivas via comunicações criptografadas.
- Atualizar a base de assinaturas de aplicações automaticamente.
- Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos.

- 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.
- 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.
- Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.
- Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.
- 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.
- 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.
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.
- Deve alertar o usuário quando uma aplicação for bloqueada.
- Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos.
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos.
- Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo.
- Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos.
- 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).
- Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação.

Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

5.10 PREVENÇÃO DE AMEAÇAS

- 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.
- Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).
- 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.
- Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade.
- 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.
- As assinaturas devem spoder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.
- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.
- Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.
- Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
- Deve permitir o bloqueio de vulnerabilidades.
- Deve permitir o bloqueio de exploits conhecidos.
- Deve incluir proteção contra ataques de negação de serviços.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de padrões de estado de conexões.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise heurística.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation.
- Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.
- Detectar e bloquear a origem de portscans.
- Bloquear ataques efetuados por worms conhecidos.
- Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.

- Possuir assinaturas para bloqueio de ataques de buffer overflow.
- Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.
- 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.
- Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.
- Identificar e bloquear comunicação com botnets.
- 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.
- Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação.
- Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.
- Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.
- Os eventos devem identificar o país de onde partiu a ameaça.
- Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
- Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 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.
- O Firewall deve permitir que se analise a implantação de Tecido de Segurança para identificar potenciais vulnerabilidades e destaque as práticas recomendadas que podem ser usadas para melhorar a segurança e o desempenho geral da rede.
- Caso o firewall possa ser coordenado por software de segurança do computador do usuário final (laptop, desktop, etc.) deve ter um perfil onde se possa executar a análise de vulnerabilidade nestes equipamentos de usuário e assegurar que estes executem versões compatíveis.
- Análise de postura de segurança devem existir para permitir que o software de segurança do endpoint aplique proteção em tempo real, antivírus, filtragem da Web e controle de aplicativos no endpoint.
- Fornecer proteção contra ataques de dia zero por meio de estreita integração com os componentes Security Fabric, incluindo NGFW, Sandbox (on-premise e nuvem).

5.11 FILTRO DE URL

- Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).
- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.
- 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.
- Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.
- Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs.
- Possuir pelo menos 60 categorias de URLs.
- Deve possuir a função de exclusão de URLs do bloqueio, por categoria.
- Permitir a customização de página de bloqueio.
- 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).
- Além do Explicit Web Proxy, suportar proxy Web transparente.

5.12 IDENTIFICAÇÃO DE USUÁRIOS

- 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.
- 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.
- Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2.
- 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.

- Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
- Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.
- 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).
- 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.
- Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.
- Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução.
- Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

5.13 QoS E TRAFFIC SHAPING

- 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 máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.
- Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem.
- Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino.
- Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo.
- Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus.
- Suportar a criação de políticas de QoS e Traffic Shaping por porta.
- O QoS deve possibilitar a definição de tráfego com banda garantida.
- O QoS deve possibilitar a definição de tráfego com banda máxima.
- O QoS deve possibilitar a definição de fila de prioridade.
- Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
-

- Suportar marcação de pacotes Diffserv, inclusive por aplicação.
- Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping.
- Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

5.14 FILTRO DE CONTEÚDO

- Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc).
- Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos.
- Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

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.

5.15 GEOLOCALIZAÇÃO

- Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado Pais/Países sejam bloqueados.
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
- Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

5.16 1VPN IPSec

- Suportar VPN Site-to-Site e Cliente-To-Site.
- Suportar IPSec VPN.
- Suportar SSL VPN.
- A VPN IPSEc deve suportar 3DES.
- A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.
- A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.
- A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).
- A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard).
- A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.
- Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
- Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting.

- A VPN SSL deve suportar o usuário realizar a conexão por meio de ciiente instalado no sistema operacional do equipamento ou por meio de interface WEB.
- A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.
- 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.
- Atribuição de DNS nos clientes remotos de VPN.
- Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.
- Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local.
  - Suportar leitura e verificação de CRL (certificate revocation list).
  - Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.
  - Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Antes do usuário autenticar na estação.
  - Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Após autenticação do usuário na estação.
  - Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Sob demanda do usuário.
  - Deverá manter uma conexão segura com o portal durante a sessão.
  - O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior).

- **DOS LOCAIS DE PRESTAÇÃO DO SERVIÇO**

Órgão deverá disponibilizar a relação dos endereços e velocidades que deverão ser entregues na solução.

7. DOS PRAZOS DE EXECUÇÃO DOS SERVIÇOS

7.1 ELABORAÇÃO DO PLANO DE IMPLANTAÇÃO

- A CONTRATADA deverá apresentar um Plano de Implantação em no máximo 10 (dez) dias corridos a partir da assinatura do Contrato.
- A execução do Plano de Implantação somente poderá ser iniciada após a sua aprovação pela CONTRATANTE.

- O detalhamento do Plano de Implantação deverá conter no mínimo:
- Cronograma com macro atividades a serem desenvolvidas para a implantação de todos os serviços previstos neste Termo de Referência. O cronograma deverá conter as seguintes informações:
  - Identificação dos responsáveis das atividades.
  - Duração das atividades.
  - Sequenciamento das atividades.
- Projeto com topologias (física e lógica) da rede, elementos envolvidos, localização dos POPs, faixas de endereçamento IP, detalhamento da gerência, bem como a arquitetura do serviço, incluindo a estratégia de roteamento.

8. DA INSTALAÇÃO DOS SERVIÇOS

- A CONTRATADA terá até trinta (30) dias corridos após a assinatura do contrato para instalar os serviços especificados no Edital e Termo de Referência.
- A instalação do circuito e CPE somente será considerada concluída após a aprovação, pelo Gestor do Contrato, que ocorrerá em até 5 (cinco) dias corridos após notificação da CONTRATADA.
- Todos os equipamentos deverão suportar alimentação com tensão de 110/220 Volts (corrente alternada) bifásica com frequência de 60 Hz.

9. DO GERENCIAMENTO DA IMPLANTAÇÃO

- Disponibilizar e alocar 1 (um) profissional que será responsável pelo gerenciamento das atividades do projeto de implantação, por parte da CONTRATADA.
- Obter informações e esclarecimentos necessários para que possa elaborar o Plano de Implantação do Serviço. Serão abordados e discutidos os seguintes pontos:

a) Instalação dos circuitos.
b) Datas e horários de restrição para implantação.
c) Requisitos de infraestrutura necessários para a instalação dos equipamentos.
d) Requisitos para a elaboração e entrega do Plano de Implantação do Serviço.
e) Serviços que deverão ser configurados na implantação.
f) Demais assuntos de interesse correlatos à implantação dos serviços.

- Apresentar ao Gestor do Contrato do CONTRANTE o(s) profissional(is) que atuará(ão) como preposto(s) da empresa para assuntos relativos à execução contratual, e informar ao CONTRANTE o nome completo e o CPF deste(s) preposto(s).

10. CENTRAL DE ATENDIMENTO E SUPORTE TÉCNICO

- A fim de manter os serviços em funcionamento adequado aos parâmetros contratuais, a CONTRATADA deverá:
- Possuir um Centro de Operações de Rede (Network Operations Center – NOC) disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável por monitorar o funcionamento dos serviços e realizar as ações corretivas necessárias para restabelecer a normalidade dos serviços.
- Possuir uma equipe especializada (SOC - Security Operation Center), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável pelo monitoramento, detecção e mitigação de ataques, realizando as ações corretivas necessárias para garantir o bom funcionamento dos serviços.
- Possuir uma equipe especializada (SOC - Security Operation Center), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável pelo monitoramento, detecção e mitigação de ataques, realizando as ações corretivas necessárias para garantir o bom funcionamento dos serviços.
- A CONTATADA deverá disponibilizar à CONTRATANTE uma Central de Atendimento Técnico, acessível via chamada telefônica gratuita (0800), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável por prestar suporte técnico, receber chamados de serviços e prestar informações acerca do andamento destes.
- O limite de atuação da CONTRATADA para fins de manutenção, reparo e configuração será a porta LAN de seus roteadores ou switches, de forma a garantir os níveis de serviço contratados.
- Enviar à CONTRATANTE, por e-mail, notificações de abertura, andamento e fechamento de chamados, realização de manutenção preventiva ou corretiva e fatos relevantes para a prestação e utilização dos serviços.
- Enviar à CONTRATANTE, por e-mail, uma lista de recorrência ("escalation list") contendo os nomes, números de telefone e endereços de e-mail das pessoas que devem ser acionadas em caso de problemas no atendimento técnico. A lista de recorrência deverá ser mantida atualizada e sua versão mais recente deverá ser enviada à CONTRATANTE sempre que houver alteração.

- A CONTRATADA deverá iniciar o atendimento no prazo máximo de 1 (uma) hora, contada a partir da data e hora do chamado.
- Todo acesso às instalações da CONTRATANTE por pessoal técnico da CONTRATADA, ou de seu preposto, deverá ser previamente agendado.
- Manutenções e/ou intervenções programadas nos serviços, quando necessárias, mesmo no caso daquelas que não impliquem inoperância dos serviços contratados ou alteração nas suas características, que necessitem a presença do técnico da CONTRATADA, deverão ser autorizadas pela CONTRATANTE.
- Qualquer manutenção e/ou intervenção de caráter emergencial para solução de falhas, inoperâncias e/ou indisponibilidades, verificadas na rede, deverá ser agendada e acordada previamente com a CONTRATANTE.

11. PORTAL DE GERENCIAMENTO E ACOMPANHAMENTO DOS SERVIÇOS

- A CONTRATADA deverá disponibilizar um Portal WEB de gerência, possibilitando a visualização online dos serviços prestados, como também realizar o registro e acompanhamento dos chamados.
- **Consulta e visualização online:** O Portal deverá apresentar informações relativas aos ativos de rede utilizados com as seguintes funcionalidades:

a) Alertas em caso de falhas e anormalidade dos circuitos.

b) Topologia da rede, incluindo roteadores e circuitos, com a visualização do status de todos os elementos.

c) Visualização da utilização de banda dos circuitos, de forma diária, semanal e mensal, com a opção de consulta de dados históricos de até 3 (três) meses.

d) Visualização do consumo de CPU e memória dos roteadores.

e) Indicação da taxa de perda de pacotes, latência e disponibilidade nos circuitos.

f) Inventario dos roteadores contendo a configuração física de cada equipamento (interfaces, memoria, cpu, etc). modelo e fabricante. endereços IPs e máscaras.

- **Registro e acompanhamento dos chamados:**

Permitir o acompanhamento dos registros de problemas e das ações executadas para a recuperação dos serviços, relativos à pelo menos aos últimos 90 (noventa) dias, incluindo as seguintes informações:

- Identificação do registro (número de chamado).
- Data e hora de abertura do chamado (registro).
- Descrição do problema.
- Identificação do reclamante (nome e telefone).
- Data e hora de conclusão do atendimento (fechamento do chamado).
- Ações realizadas para a solução do problema.

12. GERENCIAMENTO PROATIVO

A CONTRATADA deverá prover o gerenciamento proativo, com funcionamento 24 horas por dia, 7 (sete) dias na semana, incluindo sábados, domingos e feriados. Entende-se por gerenciamento proativo a capacidade da CONTRATADA de detectar falhas ocorridas nos circuitos (serviços e equipamentos) de forma autônoma e independentemente de notificação por parte da CONTRATANTE. Da mesma forma autônoma a CONTRATADA deve dar início aos procedimentos de correção de falhas e em seguida informar a CONTRATANTE sobre o evento. A CONTRATADA deverá notificar a CONTRATANTE através de telefones e e-mails definidos pela CONTRATANTE no prazo máximo de 25 minutos após a identificação do incidente.

- Gerência exclusiva de relacionamento para acompanhamento, apresentação da evolução e gestão da rede, que fará mensalmente o agendamento e apresentação dos relatórios, através de videoconferência ou por e-mail.
- Atividades realizadas pela equipe responsável pelo gerenciamento proativo:

a) Gerenciamento individualizado da rede.
b) Relatórios mensais sobre a performance da rede.
c) Relatório Gráfico de indisponibilidade.
d) Relatório de tráfego de qualidade.
e) Relatório de Consumo de Banda.
f) Relatório de Eventos ocorridos.
g) Relatório de Disponibilidade dos serviços.
h) Gerenciamento de desempenho proativo.

13. DISPONIBILIDADE

- Índice de Disponibilidade:
- Os circuitos de comunicação deverão estar disponíveis 24 horas por dia, todos os dias do ano.
- A CONTRATADA deverá garantir disponibilidade mensal de no mínimo, 99,5% para cada circuito fornecido à CONTRATANTE, calculada da seguinte forma:

DMA = [(43200 - TTICM) / 43200] x 100

Onde:
TTICM: Tempo Total de Interrupção do Circuito (em minutos) no Mês.
DMA(%): Disponibilidade Mensal Atingida

- Para efeito de cálculo de TTICM, será considerado o período em minutos entre o primeiro minuto do primeiro dia e o último minuto do último dia do calendário do mês a que se refere a fatura.
- O serviço será considerado indisponível quando não for possível a conexão entre o equipamento da CONTRATANTE e o da CONTRATADA, a partir do registro do chamado técnico na Central de Atendimento da CONTRATADA, sendo considerado disponível após o fechamento do chamado técnico, com a devida anuência da CONTRATANTE, na Central de atendimento da CONTRATADA.
- Entende-se como início do atendimento a primeira mensagem trocada pela CONTRATANTE com a CONTRATADA informando a ocorrência ou início da ligação efetuada a central de atendimento da CONTRATADA independentemente do atendimento do operador.
- O prazo máximo de recuperação dos circuitos será 2 (duas) horas, todos os dias do mês, inclusive sábados, domingos e feriados.
- As indisponibilidades informadas pela gerência e supervisão da CONTRATADA, bem como os registros na Central de Atendimento da CONTRATADA serão validadas pelos sistemas de gerência e supervisão da CONTRATANTE.
- No caso de interrupção programada por necessidade da CONTRATANTE, a mesma não afetará o índice de disponibilidade da CONTRATADA.
- As interrupções programadas solicitadas pela CONTRATANTE serão previamente combinadas com a CONTRATADA.

14. DESCONTO POR INTERRUPÇÃO:

- Para cada interrupção do circuito que for comprovadamente de responsabilidade da CONTRATADA, será calculado um desconto referente ao tempo de interrupção desse circuito, cujo valor apurado será ressarcido à CONTRANTANTE na Nota Fiscal/Fatura dos serviços com vencimento no mês seguinte ao da apuração.
- O valor do desconto será obtido a partir do seguinte cálculo:

VD = (VC / 43200) x n

Onde:

VD = Valor do Desconto
VC = Valor mensal pago pelo circuito ativo
n = Quantidade de minutos em que o serviço ficou interrompido.

- **NÍVEIS MÍNIMOS DE SERVIÇO**

A CONTRATADA deverá fornecer o serviço com os seguintes níveis mínimos de disponibilidade, latência e taxa máxima de erro, os quais são utilizados para mensurar o desempenho e a qualidade dos circuitos:

Métrica	**Nível Mínimo de Serviço**
Disponibilidade do circuito IP	>= 99,5%
Latência	<= 1ms
Perda de pacotes	<=2%

DA VINCULAÇÃO À PROPOSTA E TERMO DE REFERÊNCIA

A CONTRATADA deverá ainda executar os serviços conforme especificações constantes no Termo de Referência do Processo Seletivo em referência e da proposta apresentada, que passam a integrar o presente contrato.

QUADRO 04 – DOS VALORES

CONDIÇÕES DE PAGAMENTO: Os serviços serão pagos de forma mensal.

VALOR MENSAL: R$ XXX

VALOR TOTAL DA CONTRATAÇÃO: A contratação se refere a um valor total de xxx considerando o tempo previsto do contrato de 12 (doze) meses podendo este valor variar para mais ou para menos desde que devidamente justificável.

QUADRO 05 – CONTEÚDO DA NOTA FISCAL
CONTRATO DE GESTÃO Nº 1095/2018 –SEL
CONTRATO DE NA PRESTAÇÃO DE SERVIÇOS DE INTERNET
PERÍODO DE COMPETÊNCIA
SERVIÇO PRESTADO NO HOSPITAL MUNICIPAL DE APARECIDA DE GOIÂNIA – HMAP

As partes, devidamente qualificadas no **Quadro 01**, resolvem de comum acordo celebrar o presente instrumento nos seguintes termos e condições.

CLÁUSULA 1ª

A **CONTRATADA** obriga-se a prestação dos serviços discriminados e nas condições estabelecidas no **Quadro 03**, obrigando-se a **CONTRATANTE** a efetuar o pagamento dos serviços nos valores convencionados no **Quadro 04**. Tudo nos termos do termo de referência e da proposta da **CONTRATADA**, que são parte integrante do presente instrumento de ajuste.

CLÁUSULA 2ª

São obrigações da **CONTRATANTE**:

a) Efetuar o pagamento no prazo estabelecido, observando-se a totalidade ou parcialidade dos serviços prestados.
b) Prestar as informações necessárias para o melhor cumprimento deste Contrato.
c) Exigir a observação das normas emanadas pelos órgãos de fiscalização e controle.
d) Glosar do valor contratado eventuais prejuízos causados pela CONTRATADA, empregados e prepostos, de qualquer natureza, bem como valores decorrentes de passivos trabalhistas e fiscais gerados e não adimplidos pela **CONTRATADA**.

2.2 A **CONTRATANTE** deverá aplicar, em caso de inexecução total ou parcial das obrigações inerentes à **CONTRATADA:**

I. Advertência;
II. Multa no valor 10% do valor mensal do contrato ou valor do bloco (se for o caso).
III. Suspensão temporária da participação em outros processos seletivos no máximo de 06 (seis) meses, desde que já tenha havido aplicação da sanção prevista no inciso I por pelo menos duas vezes.

2.3. Será garantida a prévia defesa

CLÁUSULA 3ª

São obrigações da **CONTRATADA:**

a) Prestar serviços, dentro dos padrões de qualidade e eficiência exigidos para o serviço e nos dispositivos legais e convencionais impostos.
b) Respeitar, por si e por seus prepostos, as normas atinentes ao funcionamento da unidade e aquelas relativas ao objeto do presente Contrato.
c) Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, o objeto do presente instrumento, nem subcontratar quaisquer das prestações a que está obrigada. **Salvo mediante anuência expressa da Contratante quanto aos termos do ajuste.**
d) Promover a cobrança dos valores decorrentes do presente contrato somente após o respectivo vencimento e da demonstração do repasse dos valores por parte do Poder Público subscritor do Contrato de Gestão.
e) Responder por qualquer prejuízo que seus empregados ou prepostos causarem ao patrimônio da unidade ou a terceiros, decorrente de ação ou omissão culposa ou dolosa, procedendo imediatamente os reparos ou indenizações cabíveis e assumindo o ônus decorrente.
f) Manter no curso do contrato a sua regularidade fiscal e qualificação técnica exigível para o desempenho do objeto contratual
g) Manter o mais absoluto sigilo e confidencialidade no tocante aos serviços, documentos, pesquisas, entrevistas e demais informações apuradas ou de que tome conhecimento durante a relação contratual.
h) Sanar eventuais irregularidades ou correções apontadas pela CONTRATANTE quanto à apresentação de relatórios e/ou de cada etapa dos serviços.
i) Providenciar a emissão de notas fiscal de acordo com os termos contratados, **até o dia 25** do mês da efetiva prestação do serviço, no qual deverá vir instruído com os seguintes documentos, sob pena de retenção do pagamento até regularização: 1 - Certidões de Regularidades Fiscais Federais (Conjunta, CRF e Previdenciária), 2 - Municipal (ISSQN), 3 - Estadual (ICMS), 4 - Trabalhista (TST), 5 - comprovante de recolhimento do INSS e empregados, 6 – comprovante de recolhimento do FGTS dos empregados, 7 – registro de frequência dos empregados e dos sócios caso esses sejam executores da prestação de serviços, 8 – comprovante de quitação da folha de pagamento do mês trabalhado e de referência à nota fiscal emitida, 9 – relatório de produção ou relatório de serviços prestados (papel timbrado da CONTRATADA, assinatura do sócio ou representante legal).
j) Impedir o acesso à unidade de pessoa que não seja membro de seu corpo técnico com o fim de trabalhar, estagiar ou realizar qualquer atividade similar.
k) Prestar esclarecimentos no prazo designado pela CONTRATANTE em relação a qualquer procedimento de sua responsabilidade e subordinar-se às sindicâncias instauradas para averiguação de qualquer fato que tenha participado ou tenha conhecimento.
l) Acatar as glosas, sem prejuízos de advertências, caso os serviços estejam em desacordo com o contratado.
m) Cumprir de forma integral e satisfatória tudo o que consta no Termo de Referência, bem como a proposta apresentada no certame.

PARÁGRAFO ÚNICO – A perda da regularidade fiscal e/ou trabalhista no curso deste contrato, ensejará a retenção dos pagamentos até que a situação seja regularizada.

CLÁUSULA 4ª

Os serviços prestados pela **CONTRATADA** serão pagos mensalmente r e de acordo com o convencionado no **Quadro 04.**

§ 1ª – Não serão efetuados quaisquer pagamentos enquanto perdurar pendência de liquidação de obrigações impostas à **CONTRATADA** ou inadimplência contratual.

§ 2ª – Os pagamentos serão realizados unicamente por meio de depósito bancário, não sendo aceito pagamentos das faturas ou boletos bancários.
§ 3ª – O pagamento será efetuado em até 30 (trinta) dias, contados a partir do aceite da Nota Fiscal correspondente, desde que tenha havido o repasse do **Contrato de Gestão n .1095/2018 -SEL** referente ao mês da efetiva prestação de serviços por parte da Município de Aparecida de Goiânia por intermédio do Fundo Municipal de Saúde, e estará condicionado ao cumprimento integral dos serviços
§ 4ª –As Notas Fiscais deverão especificar em seu descritivo o conteúdo demonstrado no **Quadro 05** sob pena de retenção do pagamento até regularização.
§ 5ª – Do pagamento efetuado a empresa contratada serão calculados e deduzidas as retenções tributárias correspondentes conforme o tipo de serviço e o local onde esta sendo prestado.
§ 6ª – Para o caso específico do ISSQN caberá à **CONTRATADA** observar a legislação do município da prestação dos serviços.

CLÁUSULA 5ª

O contrato poderá ser reajustado ou aditivado a qualquer tempo, em razão da necessidade e sua devida comprovação justificada ou conveniência de continuação da prestação dos serviços, a partir de negociação acordada entre as partes, devidamente justificada mediante aditivo expresso.

PARÁGRAFO PRIMEIRO: Os índices de reajuste serão previstos no Termo de Referência, e na inércia da previsão será adotado o índice IGPM ou quando não aplicável será aquele que seja mais benéfico à CONTRATANTE. Os índices só poderão ser concedidos somente após 12 (doze) meses de vigência.

PARÁGRAFO SEGUNDO: Nas hipóteses de aditivos qualitativos e quantitativos serão obedecidas as seguintes regras:

a) Manutenção da natureza do objeto do contrato;
b) Manutenção das mesmas condições contratuais.

CLÁUSULA 6ª

O fiscal do Contrato designado pela **CONTRATANTE**, atestará a aceitação da entrega do serviço prestado e promoverá o aceite da nota fiscal observados os requisitos estabelecidos neste contrato, inclusive em relação ao cumprimento das metas e serviços contratados.

CLÁUSULA 7ª

Constituem motivos de rescisão unilateral pela **CONTRATANTE**:

a) O cumprimento parcial ou o não cumprimento dos serviços contratados e ou fornecimento parcial dos produtos adquiridos.
b) A desobediência de cláusulas contratuais, especificações e prazos pela CONTRATADA, ou a lentidão do seu cumprimento.
c) Atraso injustificado no início dos serviços.
d) Paralisação dos serviços.
e) O cometimento de falhas na execução do objeto do contrato.
f) Término do Contrato de Gestão, sem direito a qualquer indenização a **CONTRATADA**.
g) Ineficiência na execução do objeto contratual.
PARÁGRAFO PRIMEIRO - Nos casos em que haja descumprimento total ou parcial do objeto deste contrato a

CONTRATANTE notificará a CONTRATADA para apresentar justificativa ou sanar as deficiências no prazo máximo de 02 (dois) dias úteis, sob pena de não o fazendo o contrato ser rescindido de plano, independentemente de qualquer outra notificação.

PARÁGRAFO SEGUNDO – Garantida a defesa prévia da CONTRATADA, a CONTRATANTE poderá, além de outras medidas tendentes a regularização do contrato:

a) Aplicar advertência;
b) Suspender a execução contratual;
c) Rescindir o contrato;
d) Impedir mediante justificativa a CONTRATANTE de participar de novos processos seletivos por 06 (seis) meses.

CLÁUSULA 8ª

Poderão **AMBAS AS PARTES** sem justo motivo rescindir o presente contrato notificando com antecedência de **30 (trinta) dias.**

PARÁGRAFO PRIMEIRO: Este contrato será obrigatoriamente rescindido em caso de término do contrato de gestão.

PARÁGRAFO SEGUNDO: Caso a CONTRATANTE dispense os serviços a serem prestados durante os 30 (trinta) dias referenciados no caput, a CONTRATADA somente terá direito ao pagamento indenizatório dos referidos dias desde efetivamente preste os serviços de acordo com a manifestação do fiscal do contrato.

CLÁUSULA 9ª

A **CONTRATADA** por si e por seus sócios, administradores, gestores, representantes legais, empregados, prepostos e subcontratados ("Colaboradores"), se compromete a adotar os mais altos padrões éticos de conduta na condução dos seus negócios e não pagar, prometer ou autorizar o pagamento de qualquer valor ou oferecer qualquer tipo de vantagem indevida direta ou indiretamente, a qualquer Funcionário Público ou a terceira pessoa, bem como garante que não emprega e não empregará, direta ou mediante contrato de serviços ou qualquer outro instrumento, trabalho escravo, trabalho infantil.

CLÁUSULA 10ª

A **CONTRATADA** declara, sob as penas da lei, que não esteve envolvida com qualquer alegação de crime de lavagem de dinheiro, delito financeiro, financiamento de atividades ilícitas ou atos contra a Administração Pública, incluindo, mas não se limitando a corrupção, fraude em licitações, suborno ou corrupção e que durante a prestação dos serviços ora avençado, cumprirá com todas as leis aplicáveis à natureza dos serviços contratados, em especial a Lei de Improbidade Administrativa e Lei Brasileira Anticorrupção.

CLÁUSULA 11ª

Havendo inadimplência no repasse financeiro do Contrato de Gestão em referência pelo o ente Público, que inviabilize alguma atividade do contrato temporariamente, será permitida a SUSPENSÃO temporária e por prazo indeterminado do presente contrato, a critério do CONTRATANTE, sem direito a qualquer indenização reparatória.

PARÁGRAFO ÚNICO: A Suspensão deve ser expressamente comunicada à outra parte, com exposição dos motivos que a ensejaram, estabelecendo as partes que a simples correspondência, mediante recibo, ou envio por e-mail é suficiente para tanto.

CLÁUSULA 12ª

Fica acordado entre as partes que qualquer documentação administrativa ou judicial somente terá validade se encaminhada para o seguinte endereço: **Rua Av. Areião, Qd. 17, Lt. 23, CEP: 74820-370, Setor Pedro Ludovico, Goiânia – Goiás**.

CLÁUSULA 13ª

As partes se comprometem a agir de modo leal, responsável e probo, atuando com boa-fé para repelir quaisquer ações intencionalmente desleais, injustas, desonestas, prejudiciais, fraudulentas ou ilegais, sempre ancorados nas ações de transparência pública.

CLÁUSULA 14ª

Para dirimir as questões oriundas do presente contrato é competente o Foro da Comarca de Goiânia (GO).

Para firmeza e como prova de haverem entre si, justos e avençados, e depois de lido e achado conforme, as partes assinam o presente Contrato, em 03 (três) vias de igual teor e forma.

Goiânia (GO), _____ de _____ de 2019.

CONTRATANTE	CONTRATADA
_____ **ESTÊVÃO COSTA DALTRO** **SUPERINTENDENTE** **INSTITUTO BRASILEIRO DE GESTÃO HOSPITALAR-IBGH**	_____ **xxx**