Governo do Estado de Roraima

"Amazônia: patrimônio dos brasileiros"

CONTRATO

CONTRATO DGOF/CBMRR Nº 0361133

Contrato administrativo que entre si celebram o CORPO DE BOMBEIROS MILITAR DE RORAIMA e a empresa OI MÓVEL SA, cujo objeto é a contratação de empresa especializada na prestação de serviço de comunicação de dados terrestre por fibra óptica, para acesso a serviços da rede mundial de computadores (Internet), incluindo circuitos dedicados de comunicação de dados (locação de equipamentos, gerenciamento com suporte e solução de problemas); solução integrada de segurança (anti DDoS e Firewall UTM); solução de videoconferência; e solução de gerenciamento e distribuição da rede sem fio (controladora e pontos de acesso) conforme especificações descritas neste Termo de Referência e seus anexos, visando atender as demandas do Corpo de Bombeiros Militar de Roraima.

O Corpo de Bombeiros Militar de Roraima, pessoa jurídica de direito público, com sede na Avenida Venezuela, 1271, Pricumã, CEP nº 69.309-690, Boa Vista-RR, inscrita no CNPJ/MF sob o nº 84.012.012/0001-26, neste ato representado pelo seu Comandante Geral, CEL QOCBM **JEAN CLAUDIO** DE SOUZA HERMÓGENES, brasileiro, casado, funcionário público estadual, portador da C.I. nº 73313 e do CPF nº 323.520.342-72, residente e domiciliado na cidade Boa Vista-RR, neste ato denominado simplesmente de CONTRATANTE e, de outro lado, a empresa OI MÓVEL S/A, pessoa jurídica de direito privado, regularmente inscrita no CNPJ/MF sob nº 05.423.963/0001-11, com endereço sede, neste ato representada pelo Sr. Sr. Raul Luiz Martins Peregrino brasileiro, Solteiro, Executivo de Negócios, portador da cédula de identidade nº 22590609 SSP/AM e do C.P.F. nº 690.186.691-72 e Sr. Brasil Dias de Souza, brasileiro, casado, Executivo de Negócios, portador da cédula de identidade nº 47933 SSP/RR e do C.P.F. nº 164.042.049-68, denominada simplesmente de CONTRATADA, firmam o presente contrato nos termos do Processo Administrativo nº 19102.001220/2020.92, têm como justos, pactuados e contratados este ajuste, nos termos constantes da Lei Federal n° 8.666/93 de 21.06.93, Lei Federal nº 10.520/2002 e suas respectivas alterações posteriores:

CLÁUSULA PRIMEIRA – DO OBJETO

1. O presente contrato tem por objeto a contratação de empresa especializada na prestação de serviço de comunicação de dados terrestre por fibra óptica, para acesso a serviços da rede mundial de computadores (Internet), incluindo circuitos dedicados de comunicação de dados (locação de equipamentos, gerenciamento com suporte e solução de problemas); solução integrada de segurança (anti DDoS e Firewall UTM); solução de videoconferência; e solução de gerenciamento e distribuição da rede sem fio (controladora e pontos de acesso) conforme especificações descritas neste Termo de Referência e seus anexos, visando atender as demandas do Corpo de Bombeiros Militar de Roraima, que deriva da Ata de Registro de Preços nº 002/2020/UNEMAT, decorrente do PREGÃO PRESENCIAL SRP nº 001/2019/UNEMAT, em conformidade com o Termo de Referência apresentado e demais anexos, independente de transcrição.
1. Vinculam-se ao presente Contrato, independentemente de transcrição, o Edital do Pregão Presencial nº 001/2019/UNEMAT com seus anexos e proposta contratada.

CLÁUSULA SEGUNDA – DAS ESPECIFICAÇÕES E QUANTIDADES DOS SERVIÇOS

2. Os valores poderão eventualmente sofrer revisão (aumento ou decréscimos) nas seguintes hipóteses:
    1. Para mais, visando restabelecer o equilíbrio econômico-financeiro inicial do contrato, na hipótese de sobrevir fatos supervenientes imprevisíveis, ou previsíveis, porém, de conseqüências

incalculáveis, retardadores ou impeditivos da execução do ajustado, ou ainda, em caso de força maior caso fortuito, fato do príncipe e fato da administração, nos termos do art. 65, II, “d” e § 5º da Lei 8.666/93;

2. Para menos, na hipótese do valor contratado ficar muito superior ao valor do mercado ou quando ocorrer o fato do príncipe previsto no art. 65, § 5º da Lei 8.666/93.

2. A revisão de preços será feita com fundamento em planilhas de composição de custos e/ou preço de mercado.

2. Nos preços infracitados estão incluídas todas as despesas relativas ao objeto contratado (tributos, seguros, encargos sociais, etc.).

2. Os preços para os serviços contratados são os constantes da proposta apresentada no pregão, conforme discriminação abaixo:

Item	Especificação	Unid.	Quant. Total 12 meses	Quant. Estimado Anual	Valor Unitário R$	Valor total estimado anual R$	Valor Total 12 meses R$
5	SERVIÇO DE COMUNICAÇÃO DE DADOS TERRESTRE VIA FIBRA ÓPTICA PARA ACESSO À INTERNET COM GARANTIA TOTAL DA BANDA CONTRATADA; LARGURA DE BANDA: 100 MBPS (MEGABITS POR SEGUNDO). MENSAL.	MN	12	12	**7.674,50**	**92.094,00**	**92.094,00**
VALOR TOTAL							**92.094,00**

CLÁUSULA TERCEIRA – DO FORNECIMENTO, DOS PRAZOS E DA EXECUÇÃO DO CONTRATO

3. O contrato deverá ser executado fielmente pelas partes, de acordo com cláusulas contratuais e as normas da lei 8.666/93, respondendo cada uma pelas consequências de sua inexecução total ou parcial;

A execução do contrato deverá ser acompanhada e fiscalizada por um representante da Administração especialmente designado, nos termos do Art. 67 da Lei 8.666/93.

3. A entrega dos objetos ora contratados será acompanhada e fiscalizada por representante da Contratante, com atribuições específicas.

3. A fiscalização exercida na entrega dos bens não exclui a responsabilidade da Contratada, por quaisquer irregularidades resultantes de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência deste, não implica co-responsabilidade da Contratante ou de seus agentes e prepostos.

3.1 DO FORNECIMENTO

1. A Contratada deverá fornecer os produtos e serviços em conformidade com a especificação técnica que consta no item 1.3 deste contrato.
2. O fornecimento deverá ser realizado após a emissão da autorização da prestação de serviços, emitido pelo fiscal deste contrato.
3. O fornecedor ficará obrigado a atender todos os pedidos efetuados durante a vigência desta Ata, mesmo que a entrega deles decorrente estiver prevista para data posterior à do seu vencimento.
4. Os materiais deverão ser entregues acompanhados da Nota Fiscal ou Nota Fiscal Fatura correspondente.
5. Requisitos mínimos obrigatórios na prestação continuada dos serviços.

REQUISITOS OBRIGATÓRIOS	**REFERÊNCIA MÍNIMA**
I. Tipo de acesso – Especifica o tipo da conexão da unidade remota do órgão	Internet com acesso terrestre por meio de fibra óptica.
II. Tecnologia de transmissão	WDM, ATM, SDH OU SIMILAR SUPERIOR
III. Disponibilidade de Serviço – Relação entre o tempo de operação plena e prejudicada no período de 30 dias.	99%
IV. Tempo Máximo de Retardo Admissível – O tempo máximo de retardo na comunicação unilateral entre o ponto de conexão e o roteador de borda da Proponente para um pacote de 32 bytes.	Deverá ser igual ou inferior a 100 ms
V. Banda mínima garantida – banda mínima disponível para acesso a Internet para cada um dos pontos contemplados	100% da largura SIMÉTRICA (*downstream e upstream*) de banda contratada
VI. Ativação Pós migração/Mudança de End. – Período entre a solicitação e ativação do Serviço.	Conforme Item 25 e subitens.
VII. Prazo de Manutenção – Período máximo para o restabelecimento do serviço, contado a partir do momento da abertura do chamado até a finalização do atendimento.	Atendimento em até 2 horas. Solução em até 6 horas.
VIII. Prazo Mínimo de notificação de manutenção preventiva ou atualização de recursos técnicos – Período mínimo entre a notificação do cliente pela operadora até o início da interrupção programada.	7 (sete) dias
IX. Abertura de Chamado – Disponibilidade de atendimento para solicitações de reparos, Help Desk da Empresa Contratada e discagem sem cobrança (0800) em língua portuguesa.	24x7 (00:00 às 24:00 de Segunda a Domingo)
X. Horário de Reparo – Disponibilidade de atendimento técnico a partir da abertura da chamada.	24x7 (00:00 às 24:00 de Segunda a Domingo)

XI. Quantidade de IP's – Disponibilização de IP's que serão administrados e utilizados em sistemas e demandas do CBMRR.	
XII. Sistema Web de Monitoramento	Sim (Todos os lotes)

3.2 DOS PRAZOS DE EXECUÇÃO, FORMA E LOCAIS DE ENTREGA

1. DO PRAZO E HORÁRIOS:
    1. A CONTRATADA terá prazo de 30 (trinta) dias após a assinatura do contrato para início da instalação dos circuitos;
    2. A CONTRATADA terá prazo de 90 (noventa) dias após a assinatura do contrato para entrega total e definitiva dos circuitos;
    3. Somente nos primeiros 90 (noventa) dias, contados da assinatura do contrato, poderão ser realizados recebimentos provisórios, com velocidades diferentes das quais foram contratadas, em face da CONTRATADA necessitar realizar adequações na infraestrutura lógica da localidade para que possa ser entregue a velocidade total contratada pela CONTRATANTE.
    4. As adequações necessárias para atender a demanda solicitada, devem ser comunicadas formalmente a CONTRATANTE em um prazo mínimo de 30 (trinta) dias antes do recebimento provisório.
    5. Serão consideradas velocidades proporcionais aquelas não atingirem a largura de banda contratada.
    6. Para os Serviços objetos deste Termo de Referência, o CONTRATANTE realizará o recebimento provisório, após o fechamento do relatório contendo a relação de todas as ordens de serviços fechadas no mês de apuração. Esse relatório será emitido até o quinto dia útil do mês ao período verificado para apuração dos níveis de serviços exigidos das atividades efetivamente concluídas e aceitas no mês de referência.
    7. As solicitações de aumento de banda deverão ser atendidas num prazo máximo de 45 (quarenta e cinco) dias e não deverá ser cobrado taxa para a realização deste serviço;
    8. Para atendimento das solicitações de alteração de velocidade do circuito, este prazo poderá ser acrescido de 30 (trinta) dias quando houver necessidade de alterações na composição dos acessos (acréscimo de hardware, obras civis, troca de equipamentos de terminação/instalação de novos hardwares);
    9. Para atendimento das solicitações de alteração de endereço o prazo máximo será de 45 (quarenta e cinco) dias corridos, contados a partir da solicitação. Este prazo poderá ser acrescido de 30 (trinta) dias, quando houver necessidade de alterações na composição dos acessos (acréscimo de hardware, obras civis, troca de equipamentos de terminação/instalação de novos hardwares). Nesse caso, a CONTRATADA deverá arcar com os respectivos custos de alteração da rede, desde que não seja necessário o desenvolvimento de projetos especiais para atendimento, estimulada por estar fora da área de ATB, definido pela ANATEL.

1. Após a apuração dos níveis de serviços exigidos, e de cálculo do pagamento devido, o CONTRATANTE realizará o recebimento definitivo dos serviços.

3.3 DO LOCAL

1. Os serviços serão executados nas unidades e endereços definidos no Anexo II deste Contrato.

CLÁUSULA QUARTA – DA GARANTIA CONTRATUAL

4. A CONTRATADA deverá apresentar ao CONTRATANTE, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contado da data da assinatura do contrato, comprovante de prestação de garantia correspondente ao percentual de 3% (três por cento) do valor anual atualizado do contrato, cabendo à Contratada optar por uma das seguintes modalidades:
    1. Caução em dinheiro ou em títulos da dívida pública, devendo estes ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;
    2. Seguro-garantia;
    3. Fiança bancária.
4. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

1. Prejuízos advindos do não cumprimento do objeto do contrato;
2. Prejuízos diretos causados à administração, decorrentes de culpa ou dolo durante a execução do contrato;
3. Multas moratórias e punitivas aplicadas pela Contratante à contratada.

4. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados nos itens da alínea “b”, observada a legislação que rege a matéria;
4. A garantia em dinheiro deverá ser efetuada em favor da Contratante, no Banco do Brasil, em conta corrente específica, com correção monetária, a ser indicada pela Pró-Reitoria de Gestão Financeira;
4. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.
4. No caso da garantia apresentada na modalidade fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.
4. No caso de ocorrerem alterações no valor do contrato ou prorrogação de sua vigência ou, ainda, caso a garantia seja utilizada total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a renovar ou reforçar a garantia apresentada, observando nos mesmos moldes (exigências e prazos) estabelecidos para o início da contratação, sujeitando-se inclusive às penalidades;
4. O garantidor deverá declarar expressamente que tem plena ciência dos termos do edital e das cláusulas contratuais;
4. O garantidor não é parte para figurar em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada;
4. Será considerada extinta a garantia:
    1. Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do Contratante, mediante termo circunstanciado de que a contratada cumpriu todas as cláusulas do contrato.
    2. A Contratante executará a garantia na forma prevista na legislação que rege a matéria.
    3. A garantia prestada somente será liberada após comprovação de que a contratada quitou todas as obrigações decorrentes da contratação.

CLÁUSULA QUINTA – DAS OBRIGAÇÕES DA CONTRATANTE

5. Determinar a execução do objeto quando houver garantia real da disponibilidade financeira para a quitação de seus débitos frente à Contratada, sob pena de ilegalidade dos atos.
5. Designar, servidor gestor do contrato, ao qual caberá a responsabilidade de acompanhar, fiscalizar e avaliar a execução do contrato, conforme legislação vigente.
5. Fornecer ao contratado todos os elementos e dados necessários à perfeita execução do objeto deste Contrato, inclusive permitindo o acesso de empregados, prepostos ou representantes da contratada em suas dependências, desde que observadas às normas de segurança.
5. Emitir ordem de serviço estabelecendo dia, hora, quantidade, local e demais informações que achar pertinentes para o bom cumprimento do objeto.
5. Disponibilizar local adequado para a realização da entrega.
5. Rejeitar, no todo ou em parte, os produtos entregues em desacordo com as obrigações assumidas pela Contratada.
5. Notificar a CONTRATADA de qualquer alteração ou irregularidade encontrada na execução do contrato.
5. Efetuar o pagamento à CONTRATADA, nas condições estabelecidas neste contrato e em edital.
5. Informar à CONTRATADA sobre atos que possam interferir direta ou indiretamente nos serviços prestados;

5. Forma de prestação de informações e esclarecimentos será por e-mail do fiscal técnico.

CLÁUSULA SEXTA - DAS OBRIGAÇÕES DA CONTRATADA

Prestar, por meio de seu Fiscal Técnico do Contrato, as informações e os esclarecimentos pertinentes ao(s) serviço(s) contratado(s) que venham a ser solicitados pela CONTRATADA;

6. O pagamento poderá ser efetivado até 30 (trinta) dias após a entrega da Nota Fiscal de Serviço devidamente atestada (liquidada), e com todas as certidões conforme exigências do fisco.
6. Notificar à CONTRATADA quanto a irregularidades ou defeitos verificados na execução das atividades objeto deste Termo de Referência, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para o CONTRATANTE;
6. Promover a fiscalização do contrato, sob os aspectos quantitativos e qualitativos, por intermédio de servidores designados, anotando em registro próprio as falhas detectadas e exigindo as medidas corretivas necessárias, bem como acompanhar o desenvolvimento do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes, quando comprovada a execução total, fiel e correta dos serviços, podendo ainda sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos contratuais;
6. Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações contratuais, inclusive permitir acesso aos profissionais ou representantes da CONTRATADA às dependências, quando necessário, aos equipamentos e às soluções de software do CONTRATANTE relacionados à execução do(s) serviço(s), mas com controle e supervisão das áreas técnicas do CONTRATANTE;
6. Aprovar ou rejeitar, no todo ou em parte, os produtos e serviços entregues pela CONTRATADA;
6. Aprovar ou reprovar as atualizações tecnológicas propostas pela CONTRATADA;
6. Aplicar as sanções previstas em contrato, assegurando à CONTRATADA o contraditório e a ampla defesa.
6. Responsabilizar-se pelo perfeito funcionamento do objeto da contratação. Isso significa que eventual omissão técnica constante neste documento deva ser suprida pela contratada, sem ônus adicional ao CBMRR já que em suma, o objeto da contratação é a entrega de uma de Rede de Dados funcional;
6. Assumir total responsabilidade pelo sigilo das informações e dados contidos em qualquer mídia e/ou documento que vier a ter acesso em virtude dos serviços prestados.
6. Acompanhar e cumprir os Níveis Mínimos de Serviços Exigidos na Tabela 1
6. Garantir a veracidade das informações fornecidas ao Contratante;
6. Disponibilizar central de atendimento telefônico não tarifado (0800) para registro de chamados.
6. Enviar mensalmente, ao fiscal técnico, juntamente com a Fatura, um relatório contendo a disponibilidade dos links contratados, bem como, os chamados registrados.
6. A contratada responsabiliza-se por:
    1. Selecionar e preparar rigorosamente o empregado que irá prestar os serviços;
    2. Garantir a prestação dos serviços, mesmo em estado de greve da categoria, através de esquema de emergência;
    3. Arcar com qualquer custo trabalhista em virtude da jornada de trabalho dos profissionais que vier a disponibilizar para reparo da conectividade ou suporte a fim;
    4. Implantar, de forma adequada, a planificação, execução e supervisão permanente dos serviços, de forma a obter uma operação correta e eficaz, realizando os serviços de forma meticulosa e constante, mantendo sempre em perfeita ordem a prestação dos serviços;
    5. Orientar seus empregados de que não poderão se retirar dos prédios ou instalações da Contratante portando volumes ou objetos sem a devida autorização e liberação no posto de vigilância;
    6. Dar ciência aos empregados do conteúdo do contrato e das orientações contidas neste documento;

7. Responsabilizar-se pelo cumprimento, por parte de seus empregados, das normas disciplinares determinadas pela Administração;

6. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Administração;
6. Prever toda a mão-de-obra necessária para garantir a perfeita execução dos serviços, nos regimes contratados, obedecidas às disposições da legislação trabalhista vigente;
6. Manter durante a vigência do contrato as condições de habilitação, apresentando sempre que exigido pela fiscalização, os comprovantes de regularidade fiscal;
6. Relatar à fiscalização do contrato toda e qualquer irregularidade observada na prestação dos serviços;
6. Não transferir a outrem, no todo ou em parte, a execução do contrato, sem prévia e expressa anuência desta Corte, excetuando-se os casos previstos neste documento;
6. Responder civil e penalmente, por quaisquer danos ocasionados à Administração e seu patrimônio e/ou a terceiros, dolosa ou culposamente, em razão de sua ação ou de omissão ou de quem em seu nome agir;
6. Responsabilizar-se pela conduta do empregado que for incompatível com as normas da contratante, tais como: cometimento de ato desidioso, negligência, omissão, falta grave, violação do dever de fidelidade, indisciplina no descumprimento de ordens gerais e sigilo e segurança da informação;
6. Receber as observações do Fiscal Técnico do contrato, relativamente ao desempenho das atividades, e identificar as necessidades de melhoria;
6. Registrar e controlar, diariamente, as ocorrências e os serviços sob sua responsabilidade;
6. Permitir a fiscalização e o acompanhamento da execução do objeto a ser contratado por servidor designado pelo contratante, em conformidade com o artigo 67 da Lei nº 8.666/93;
6. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessárias, nos termos do art. 65, § 1º da Lei 8.666/93;
6. Indenizar quaisquer danos ou prejuízos causados ao CBMRR ou a terceiros, por ação ou omissão do seu pessoal durante a execução dos serviços;

CLÁUSULA SÉTIMA – DA DOTAÇÃO ORÇAMENTÁRIA

7. As despesas decorrentes da aquisição/contratação, objeto desta licitação, correrão à conta da seguinte dotação orçamentária.

Órgão: 19.102

Programa: 06.182.012.2050

Elemento de Despesa: 33.90.40

Fonte: 108/308

7. As despesas decorrentes da contratação, objeto deste contrato, no exercício seguinte, correrão à conta dos recursos específicos consignados no orçamento do mesmo.

CLÁUSULA OITAVA – DO PAGAMENTO

8. O pagamento ocorrerá após a entrega ou a execução dos serviços e recebimento da fatura/nota fiscal e devidamente atestado por responsável da contratante, mediante ordem bancária, através do Banco do Brasil S/A, a ser depositada em conta-corrente, no valor correspondente em moeda corrente.
8. A contratada deverá indicar no corpo da nota fiscal/fatura, o número e nome do banco, agência e número da conta onde deverá ser feito o pagamento, via ordem bancária;

1. Caso constatado alguma irregularidade nas notas fiscais/faturas, estas serão devolvidas ao fornecedor, para as necessárias correções, com as informações que motivaram sua rejeição, contando- se o prazo para pagamento da data da sua reapresentação.
2. Nenhum pagamento isentará a fornecedora/contratada das suas responsabilidades e obrigações, nem implicará aceitação definitiva do fornecimento.

8. As notas fiscais/faturas devem ser emitidas em nome do Corpo de Bombeiros Militar de Roraima, com o seguinte endereço: Avenida Venezuela, nº 1271, Pricumã, Boa Vista-RR e deverão ser entregues no local indicado pela contratante.
8. A contratante, não efetuará pagamento de título descontado, ou, por meio de cobrança em banco, bem como, os que forem negociados com terceiros por intermédio da operação de “factoring”;
8. As despesas bancárias decorrentes de transferência de valores para outras praças serão de responsabilidade da contratada;
8. Junto às notas fiscais a contratada deverá obrigatoriamente apresentar os documentos relacionados abaixo, sem as quais fica impossibilitada a efetivação da liquidação do pagamento;

1. prova de regularidade fiscal para com a Fazenda Federal, Estadual e Municipal do domicílio ou sede da contratada, consistindo em certidões ou documento equivalente, emitidos pelos órgãos competentes e dentro dos prazos de validade expresso nas próprias certidões ou documentos;
2. prova de regularidade fiscal para com a Procuradoria da Fazenda Nacional e para com a Procuradoria Geral do Estado, nos casos em que não sejam emitidas em conjunto às regularidades fiscais;
3. prova de regularidade perante o Fundo de Garantia por Tempo de Serviço – FGTS (art. 27 da Lei 8.036/90), em plena validade, relativa à contratada;
4. prova de regularidade perante o Instituto Nacional de Seguridade Social- INSS (art. 195, § 3° da Constituição Federal), em plena validade, relativa à contratada.
    8. As comprovações de regularidade exigidas nas alíneas constantes do item anterior, poderão ser substituídas pela regularidade junto ao Cadastro Geral de Fornecedores do Estado de Roraima;

8. Constatando-se qualquer incorreção na nota fiscal, bem como qualquer outra circunstância que desaconselhe o seu pagamento, o prazo para pagamento constante do subitem acima fluirá a partir da respectiva regularização. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária;
8. Caso constatado alguma irregularidade nas notas fiscais/faturas, estas serão devolvidas ao fornecedor, para as necessárias correções, com as informações que motivaram sua rejeição, contando- se o prazo para pagamento da data da sua reapresentação;
8. Nenhum pagamento será efetuado à empresa contratada enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária;
8. O pagamento efetuado à contratante não a isentará de suas responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade e validade, nem implicará aceitação definitiva do fornecimento;
8. Não haverá, sob hipótese alguma, pagamento antecipado.
8. Deverá apresentar a nota fiscal de entrada do produto no ato da liquidação, procedimento de conferência, de acordo com o que determina a Lei nº 4.320/64, art. 3º, § 2º, I.
8. O pagamento será efetuado à contratada mediante crédito(s) em conta(s) corrente(s), até o 30º (trigésimo) dia do mês subsequente à apresentação da Nota Fiscal /Fatura devidamente atestada pelo setor responsável pelo seu recebimento e pelo servidor designado para esse fim.
8. Nenhum pagamento será efetuado à Contratada enquanto pendente de liquidação qualquer obrigação, não podendo este fato ensejar direito de reajustamento de preços ou a atualização monetária.
8. Os pagamentos não realizados dentro do prazo, motivados pela Contratada, não serão geradores de direito a reajustamento de preços.
8. Ocorrendo atraso no pagamento, e desde que para tal não tenha concorrido de alguma forma a Contratada, os valores devidos poderão ser corrigidos, mediante solicitação da Contratada, pela variação

do Índice Geral de Preços – Disponibilidade Interna- IGP-DI, coluna 2, publicada pela Fundação Getúlio Vargas, ocorrido entre a data final prevista para o pagamento até a data de sua efetiva realização.

8. O faturamento deverá ser emitido para: Corpo de Bombeiros Militar de Roraima – com o CNPJ Nº. 84.012.012/0001-26 – Inscrição Estadual: 24.901.023-8, Av. Venezuela, nº 1271, Pricumã.

8. Obrigações Acessórias para pagamento:
    1. Para efeitos de ativação de todos os links de comunicação em todas as unidades, será aceito, nos primeiros 120 (cento e vinte) dias da execução contratual contados de sua assinatura, o pagamento fracionado dos links, sendo estes proporcionais aos links que estarão recebidos pelo CBMRR.
    2. Para efeitos de pagamento parcial, poderá ser pago o valor proporcional do link recebido provisoriamente, quando a CONTRATADA apresentar justificativa da não entrega total da velocidade contratada, com antecedência mínima de 30 (trinta) dias, não podendo exceder o prazo de 120 (cento e vinte) dias da assinatura do contrato.
    3. A proporcionalidade do pagamento será estabelecida pela razão entre a velocidade especificada e a velocidade efetivamente fornecida. Por exemplo: Caso um link de 8Mb seja entregue com 2Mb durante o período de ativação, seu faturamento ocorrerá na proporção de 25 % do preço ofertado para o link de 8Mb.

1. A data de vencimento da fatura nunca poderá ser inferior a 30 dias da data de seu efetivo encaminhamento o CBMRR.
2. A fatura deverá ser encaminhada a partir do quinto dia do mês subsequente à prestação do serviço, após a apresentação do relatório do Nível Mínimo de Serviço.
3. Havendo penalidade de multa, glosas ou indenizações, o valor poderá ser deduzido do crédito que a CONTRATADA porventura fizer jus.
4. A nota fiscal deverá ser apresentada em duas vias para que possam ser atestadas e encaminhadas para pagamento, devendo conter as seguintes especificações:
    1. A data de emissão da nota fiscal;
    2. O total de links instalados, agrupados ou não por tipo de conexão;
    3. Todas as instalações (tipo de link e local) com suas respectivas datas de ativação e o valor proporcional ao número de dias de serviço de conexão efetivamente prestado - no caso das instalações, alterações de velocidade ou mudança de endereço (Quantidades e especificações do material/serviços que foi(ram) entregue(s));
    4. O valor unitário e total, de acordo com a proposta apresentada;
    5. CNPJ constante da fatura deverá ser o mesmo indicado na proposta de preços e na nota de empenho.

CLÁUSULA NONA – DA VIGÊNCIA

9.1**.** Este instrumento vigorará a partir de sua assinatura pelo prazo de 12 (doze) meses, tendo seu extrato publicado no Diário Oficial, no prazo legal.

CLÁUSULA DÉCIMA – DA RESCISÃO, DO RECONHECIMENTO DOS DIREITOS DA ADMINISTRAÇÃO PREVISTAS NO ART.77 DA LEI FEDERAL 8666/93:

10.1. O inadimplemento das cláusulas estabelecidas neste contrato pela contratada assegurará a contratante o direito de rescindi-lo, no todo ou em parte, a qualquer tempo, mediante comunicação oficial de no mínimo 30 (trinta) dias de antecedência à outra parte, em consonância com a Lei 8.666/93 e suas alterações.

CLÁUSULA DÉCIMA PRIMEIRA – DAS PENALIDADES

Rol não exaustivo de penalidades:

Tabela 4 - Rol não Exaustivo de penalidades

Penalidade	Definição/Aplicação	PENALIDADE
Descumprimento Parcial do contrato	Conforme **Tabela 5 - Descumprimento parcial**	Variável, conforme a falta/erro constatado;
Descumprimento Parcial reiterado do contrato	Reincidência do descumprimento parcial do contrato até 5 (cinco) vezes por link no mês	Multa correspondente a 1/15 (um quinze avos) do valor mensal dos links incidentes, por dia de descumprimento, limitada a 50% (cinquenta por cento) do valor mensal
Descumprimento Total do contrato **ou** Descumprimento Parcial reiterado do contrato	Não entrega do objeto deste Termo de Referência ou a Reincidência do descumprimento parcial do	Multa correspondente a 1/15 (um quinze avos) do valor mensal do contrato, por dia de descumprimento, limitada a 50% (cinquenta por cento)

		do valor mensal rescisão contratual.	do	Contrato	e

Tabela 5 - Descumprimento Parcial

SERVIÇO	REFERÊNCIA E APLICAÇÃO	PENALIDADE
Novas instalações, mudança de endereço e alteração de velocidade das Conexões (Ativações)	Atraso/descumprimento dos prazos de instalação, mudança de endereço ou alteração de velocidade de conexão.	Multa correspondente a 1/30 (um trinta avos) do valor mensal da conexão contratada em atraso, por dia de descumprimento, limitada a 10% (dez por cento) do valor mensal da contratação
Baixa qualidade da Conexão (descumprimento do NMS)	Baixa qualidade (inclusive nos casos de mudança de endereço).	Multa correspondente a 1/30 (um trinta avos) do valor mensal da conexão contratada, por hora de descumprimento do NMS e do INMS, limitado a 10% (dez por cento) do valor mensal da contratação
Solicitação de viabilidade técnica	Solicitação de viabilidade técnica para mudança da conexão – Atraso na resposta quanto à viabilidade.	Multa correspondente a 1/30 (um trinta avos) do valor mensal das viabilidades em atraso por dia de descumprimento, limitada a 10% (dez por cento) do valor mensal da contratação (VMC) com base no valor da contratação.
Violação do sigilo das informações	Condições de Sigilo.	Multa de 10% sobre o valor total da contratação.
Inatividade da conexão	Falta de disponibilidade de acesso.	Multa de 0,2% do valor mensal da conexão contratada, por hora de indisponibilidade de descumprimento do

		NMS e INMS, limitada à 10% do total do valor do Link.

11. O prazo máximo para execução da viabilidade técnica será a metade do tempo necessário para a ativação e/ou mudança de endereço, previstos nos itens 25 e subitens deste Termo de Referência, não podendo este prazo ser prorrogado ou adiado. A penalidade prevista no item 26 e subitens será aplicada no primeiro dia após a finalização do prazo citado neste item.
11. Independente de outras sanções legais e das cabíveis penais, pela inexecução total ou parcial da contratação, a administração poderá, garantida a prévia defesa, aplicar à empresa licitante, segundo a extensão da falta cometida, as seguintes penalidades, previstas no art. 87, da Lei n. 8.666/93:
11. Advertência, por escrito, nas hipóteses de execução irregular da contratação, fora dos padrões técnicos de instalação que não resulte em prejuízo para o serviço do CBMRR
11. Aplicação de multa administrativa com natureza de perdas e danos da ordem de 10% (dez por cento) sobre o valor total da contratação, nas hipóteses de inexecução total ou violação do sigilo e de 10% (dez por cento) sobre o valor mensal, se ocorrer inexecução parcial, reconhecendo a empresa os direitos deste Regional, nos termos do art. 77 da Lei nº. 8.666/93;
11. Suspensão temporária de participação em licitação e impedimento de contratar com o CBMRR, por prazo não superior a 2 (dois) anos;
11. Declaração de inidoneidade para licitar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição, ou até que seja promovida a reabilitação, na forma da lei, perante a própria autoridade que aplicou a penalidade, de acordo com o inciso IV, do art. 87, da Lei 8.666/93.
11. A critério da Administração, com fundamento no art. 7°, da Lei 10.520/2002, a empresa licitante poderá ficar impedida de licitar e contratar com o Estado pelo prazo de até 05 (cinco) anos, se,

convocado dentro do prazo de validade da sua proposta, não iniciar os serviços, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, comportar-se de modo inidôneo ou cometer fraude fiscal, sem prejuízo das multas previstas no Contrato.

11. A aplicação da sanção de suspensão e declaração de inidoneidade implica a inativação do cadastro, impossibilitando o fornecedor ou interessado de relacionar-se comercialmente com a Administração Estadual, no âmbito do SISG e dos demais órgãos/entidades que, eventualmente, aderirem ao SICAF, na forma prevista no item 6.4 da IN MARE nº. 05/95
11. Considera-se também inexecução parcial do Contrato, para fins de aplicação de penalidade, a não comprovação de manutenção das condições de habilitação e regularidade fiscal e trabalhista exigidas no certame;
11. No caso de descumprimento das demais condições previstas neste documento, no edital ou no contrato onde não haja previsão de sanções específicas, verificando-se qualquer tipo de dano ou prejuízo ao erário, poderá ser aplicada a multa de 1% por dia, incidente sobre o valor mensal da contratação até o limite de 10% (dez por cento), ou ser caracterizado descumprimento parcial da contratação, mediante processo administrativo, garantida a ampla defesa.
11. Caso o descumprimento provoque prejuízo ou dano de grande monta (Ex.: atraso na tramitação de processos, indisponibilidade do PJe, PEA, entre outros sistemas, erros em consultas processuais, violação de dados sigilosos comprovadamente ocasionados dentro da rede da operadora), poderá caracterizar o descumprimento parcial ou mesmo total da contratação.
11. As sanções serão publicadas no DOE e, obrigatoriamente, registradas no SICAF e, no caso de impedimento de licitar e contratar com o Estado/CBMRR, a licitante será descredenciada por igual período, sem prejuízo das multas previstas neste Termo.
11. Quando do início da prestação dos serviços, expirados os prazos propostos para a entrega, sem que a contratada o faça, iniciar-se-á a aplicação da penalidade de multa de mora, correspondente a 0,5% (meio por cento) por dia de atraso injustificado ou cuja justificativa não tenha sido acatada pela Administração deste Egrégio Tribunal, incidente sobre o valor total do link em atraso contratado.

11. A multa prevista neste item será aplicada até o limite de 20 (vinte) dias. Após o 20º (vigésimo) dia, os serviços poderão, a critério da Administração, não mais ser aceitos, configurando a inexecução total da contratação, com as consequências prescritas em lei, no ato convocatório e no instrumento contratual.
11. A empresa vencedora terá o prazo máximo de 10 (dez) dias úteis, após regular notificação por escrito, para assinar o contrato. Tal notificação poderá ser realizada por e-mail.
11. Caso não o faça neste prazo, poderá ser aplicada a multa de 0,3% por dia, incidente sobre o valor total da contratação até o limite de 10% (dez por cento do VTC), mediante processo administrativo, garantida a ampla defesa.
11. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.
11. Se a CONTRATADA não recolher o valor da multa que porventura lhe for imposta, dentro de 5 dias úteis, a contar da data da notificação do responsável, o valor devido será objeto de inscrição na Dívida Ativa Estadual para posterior execução judicial e/ou será passível de protesto.
11. Do ato que aplicar a penalidade, caberá recurso no prazo de 5 (cinco) dias úteis, a contar da ciência da intimação, podendo a Administração reconsiderar sua decisão, dentro do mesmo prazo.

CLÁUSULA DÉCIMA SEGUNDA – DO DIREITO DE PETIÇÃO

12.1**.** No tocante a recursos, representações e pedidos de reconsideração, deverá ser observado o disposto no art. 109 da Lei nº 8.666\93.

CLÁUSULA DÉCIMA TERCEIRA – DA FISCALIZAÇÃO E ACOMPANHAMENTO

13. **Será Designados pelo CONTRATANTE:**
    1. Equipe de Gestão da Contratação: equipe composta pelo Gestor do Contrato, Fiscal Técnico do Contrato: servidor representante da Área de Tecnologia da Informação, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos técnicos da solução;
    2. Equipe de Fiscalização: equipe composta pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares.
    3. Gestor do Contrato: servidor com atribuições gerenciais, administrativas, técnicas ou operacionais relacionadas ao processo de gestão do contrato, sendo responsável por gerir a execução consoante às atribuições regulamentares.
    4. Fiscal Demandante do Contrato: servidor representante da Área Demandante da Solução de Tecnologia da Informação, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos funcionais da solução;
    5. Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais;
    6. Fiscal Técnico do Contrato
        1. O CONTRATANTE designará servidor(es) para atuar como Fiscal Técnico do Contrato, ao qual caberão as seguintes responsabilidades:
        2. Realizar a abertura das Ordens de Serviço;
        3. Atuar como responsável técnico pela Ordem de Serviço;
        4. Acompanhar a execução de cada serviço, registrando eventuais falhas de procedimento, problemas de qualidade e rejeites de artefatos, atrasos e eventuais outros problemas inerentes à Ordem de Serviço;
        5. Avaliar a qualidade dos serviços realizados de acordo com os critérios de aceitação definidos em contrato em conjunto com os usuários requisitantes dos serviços;

6. Em razão da complexidade e volume dos serviços contratados, deverão ser designados pelo CONTRATANTE tantos Fiscais Técnicos quantos forem necessários, tendo em vista uma eficaz fiscalização e acompanhamento dos serviços contratados;

13.2.Designados pela CONTRATADA

1. Preposto: funcionário representante da Contratada, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual. Em caso de substituição do Preposto, a contratada deverá comunicar formalmente a equipe de fiscalização, via e-mail, o nome do preposto substituto.

Em caso de substituição do Preposto acima, a contratada deverá comunicar formalmente a EQUIPE DE FISCALIZAÇÃO, via e-mail, o nome do preposto substituto.

Constitui encargo exclusivo da CONTRATADA, suportar todos os ônus para a remuneração desses profissionais, bem como dos demais alocados no contrato. Assim, o CONTRATANTE não remunerará em nenhuma hipótese, sob nenhuma justificativa ou fundamento, a CONTRATADA pela atividade de representação administrativa.

O Preposto será o responsável pela gestão administrativa do contrato junto ao CONTRATANTE, responsabilizando-se por todos os recursos necessários à adequada prestação dos serviços, inclusive pela atuação dos Responsáveis Técnicos.

1. Cabe ao Preposto:
    1. Responder pela CONTRATADA;
    2. Receber as correspondências e as intimações do CONTRATANTE;

1. Assegurar que as determinações do CONTRATANTE sejam disseminadas junto aos profissionais alocados à execução dos serviços;
2. Informar o CONTRATANTE sobre problemas de qualquer natureza que possam impedir o andamento normal dos serviços;
3. Elaborar e apresentar relatórios gerenciais dos serviços demandados, contendo detalhamento dos serviços executados e em andamento e demais informações necessárias ao acompanhamento e avaliação da execução das Ordens de Serviço ou de Chamados Técnicos.

13. O exercício da fiscalização pela contratante não excluirá nem reduzirá as responsabilidades de competência da contratada.

13. As atribuições do fiscal do contrato são:

1. Conhecer detalhadamente o instrumento contratual
2. Conhecer detalhadamente o contrato e sanar qualquer dúvida com os demais setores competentes da administração para o fiel cumprimento das cláusulas neles estabelecidas:
3. Acompanhar a execução contratual, em seus aspectos quantitativos e qualitativos;
4. Registrar todas as ocorrências surgidas durante a execução do objeto;
5. Determinar a reparação, correção ou substituição total ou parcial do objeto do contrato em que se verifiquem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;
6. Rejeitar, parcial ou total o fornecimento executado em desacordo com o contrato;
7. Exigir e assegurar o cumprimento dos prazos previamente estabelecidos;
8. Exigir o cumprimento das cláusulas do contrato e respectivos termos aditivos e verificar a existência de possível subcontratação vedada contratualmente;
9. Aprovar a medição da entrega efetivamente realizada, em consonância com o regime de execução previsto no contrato.

Obs: o fiscal jamais deve atestar a prestação de serviço que não foi totalmente entregue;

10. Liberar e encaminhar as faturas ou notas fiscais;

11. Comunicar à autoridade superior, em tempo hábil, qualquer ocorrência que requeira decisões ou providências que ultrapassarem sua competência, em face de risco ou iminência de prejuízo ao interesse público;
12. Receber o objeto contratual, mediante termo circunstanciado assinado pelas partes;
13. Manter controle das notas fiscais emitidas a fim de evitar que o valor do contrato seja ultrapassado;
14. Emitir atestados de avaliação dos produtos entregues (certidões ou atestados).
15. Comunicar formalmente e com antecedência o seu afastamento das atividades de fiscalização para que assuma o substituto;
16. Solicitar, em tempo hábil e com a concordância da unidade solicitante, os aditamentos ao contrato;
17. Receber e dar o encaminhamento devido ás dúvidas ou questionamentos;
18. Confeccionar e apresentar quando solicitado relatórios circunstanciados de acompanhamento da entrega dos produtos;
    13. O fiscal deverá acompanhar os prazos do contrato, informando aos interessados e providenciando, em tempo hábil, a solicitação de aditamentos e alterações à supervisão de acompanhamento de contratos através de processo devidamente autuado e instruído com os documentos necessários disponíveis no processo SE nº 19102.001220/2020.92.
    13. O fiscal, a fim de se resguardar, deve protocolar, junto à autoridade superior, qualquer registro de dificuldade ou impossibilidade para o cumprimento de suas obrigações, com identificação dos elementos impeditivos do exercício da atividade e das providências e sugestões que porventura entender cabíveis.

CLÁUSULA DÉCIMA QUARTA – DOS REQUISITOS TÉCNICOS

14.1. Tratando-se de requisito técnico de disponibilidade dos Lotes 02 a 05, no momento da assinatura do contrato, a(s) CONTRATADA(S) deverá(ão) entregar declaração de que não fará(ão) uso da infraestrutura da outra CONTRATADA do Lote 01 para fornecimento do serviço ao CBMRR, o que será aferido pelos meios técnicos disponíveis na internet, como o sítio WWW.CIDR-REPORT.ORG, após a conexão de trânsito à Internet estar instalada e operacional;

14.2.A CONTRATADA deverá, caso seja do interesse da CONTRATANTE, estabelecer sessão BGP com a mesma, e divulgar seu ASN e prefixos IPv4 na tabela BGP global, através de todos os fornecedores da CONTRATADA;

14. Os endereços IP disponibilizados pela contratada não deverão ser da mesma faixa utilizada pelos usuários de IP's dinâmicos (ex.: Velox, GVT, etc.) ou terem sido anteriormente de faixa de endereços IP utilizados para esse fim;
14. Caso os endereços IP fornecidos pela CONTRATADA estiverem relacionados em blacklists como suspeitos de origem de spam ou algo similar (sites maliciosos), a mesma deverá fornecer outro bloco em, no máximo, 5 (cinco) dias úteis, sem qualquer ônus para o CBMRR;
14. A CONTRATADA deverá prover trânsito e rotas tanto para o protocolo IPv4 quanto para o IPv6, sem túnel ou qualquer tipo de encapsulamento, ambos através do mesmo enlace de dados;
14. A velocidade ofertada deverá ser efetiva, ou seja, deverá haver garantia de banda até o backbone IP da operadora;
14. Deverão estar inclusos na solução todos os recursos de conectividade, tais como, roteadores, modems, conversores, alimentadores DC, cabos ou outros correlatos bem como TODA a infraestrutura para instalações de equipamentos de transmissão necessárias à prestação dos serviços e à integração com o ambiente operacional do local de instalação. A infraestrutura elétrica AC, aterramento e condicionamento de ar serão de responsabilidade da CONTRATANTE;
14. Para todos os Itens do LOTE 01 - LINK IP DEDICADO COM SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO INTEGRADA, deverá ser disponibilizado, pela CONTRATADA, juntamente com a rede de comunicação de dados, os equipamentos da Solução Integrada de Segurança do tipo UTM (Unified Threat Management) que tenha a capacidade de integrar em um único dispositivo: filtro de

pacotes com controle de estado, camada de antivírus, filtro de conteúdo WEB, filtro anti-spam, VPN, IDS/IPS, balanceamento de carga, QoS e Proxy reverso e controladora Wi-FI, vinculados à contratação dos correspondentes serviços de acesso.

14. TODOS os equipamentos e enlaces fornecidos pela CONTRATADA, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área – ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações);

14. Será solicitado à futura vencedora do certame que forneça acesso ininterrupto à no mínimo 5 pessoas da Diretoria Administrativa de Tecnologia da Informação - DATI, ao sistema de monitoramento de chamados, para que o CBMRR possa acompanhar o andamento e solução do problema relatado no chamado. Neste mesmo sistema, deverá ser permitida a abertura de chamados para a empresa por parte do CBMRR, através de ferramenta web ou através de um telefone 0800.

14. O CBMRR deverá ter acesso de visualização (somente leitura – Read Only) aos roteadores de toda a estrutura da rede IP, bem como comunidades SNMP read para ambos.

    1. Para os roteadores das redes IP, as portas destes equipamentos deverão ter suas referências de velocidade (BANDWIDTH) devidamente configuradas, sendo estas velocidades iguais às contratadas.
    2. Será solicitada a revisão tecnológica dos itens descritos a cada 24 meses.
    3. Nesta revisão poderá ser solicitada a alteração de protocolos que estejam habilitados ou não;
    4. Durante o prazo de vigência do contrato, a CONTRATADA deverá garantir a atualização tecnológica necessária para a prestação dos serviços.

1. As atualizações de programas deverão cobrir todos os programas (software e firmware) de propriedade da CONTRATADA e incluir o fornecimento de correções (patches) e novas versões/revisões/distribuições (releases) assim que o fabricante as tornem disponíveis.
2. Entende-se por atualização de programas qualquer correção, pequena modificação, aperfeiçoamento (update), ou desenvolvimento de nova versão (upgrade) efetuado pelo fabricante para os produtos em questão.

14. Todos os equipamentos necessários para o funcionamento dos links de comunicação deverão ser instalados em racks da CONTRATADA, entre outros equipamentos que se façam necessários, atendendo às velocidades contratadas e o SLA.

    1. Poderão ser instalados os referidos equipamentos em local diverso do rack, contanto que esta instalação seja previamente acordada e autorizada pela CONTRATANTE.
    2. A CONTRATADA não poderá se recusar a realizar a instalação dos equipamentos para o funcionamento dos links por ausência de rack ou sistema de proteção elétrica (No-Break) para a instalação.

14.13. Serviço de proteção anti-DDoS:

1. Para todos os Itens do Lote 01, será solicitado à implementação do serviço de proteção anti-DDoS.
    1. A contratada deverá possuir mecanismos que permitam bloquear ataques DDoS (Distributed Denial of Service), mediante monitoramento, detecção e mitigação, conforme critérios mínimos abaixo:
        1. O serviço deverá ter pró-atividade para solução e prevenção de incidentes e ataques; . A CONTRATADA deverá monitorar a disponibilidade e performance em regime 24hx7d;
2. A CONTRATADA deverá tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataque de DDoS, recuperando o pleno funcionamento do mesmo;
3. A solução deve possuir a capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP;
4. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White lists, Black lists, limitação da taxa, técnicas desafio resposta, descarte de pacotes mal formados, técnicas

de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, entre outras;

5. A solução deverá implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam uso não autorizado dos recursos de rede, tanto para IPv4 quanto para IPv6, incluindo, mas não se restringindo apenas, a ataques de inundação (Flood de UDP e ICMP), ataques à pilha TCP (mal uso das flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle reset), ataques que utilizam fragmentação de pacotes (IP, TCP e UDP), ataques de BotNets e Worms, ataques que utilizam falsificação de endereços IP (IP Spoofing) e ataques à camada de aplicação (protocolos HTTP e DNS);
6. A solução 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;
7. A CONTRATADA deve possuir 2 (dois) centros de limpeza nacional, cada um com capacidade de mitigação de 500MB e 1 (um) centro de limpeza internacional com capacidade de mitigação de 5Gb;
8. A CONTRATADA deve mitigar ataques por 3 horas, caso o ataque ultrapasse o SLA de mitigação contratado;
9. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contra medidas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole;

1. A solução de detecção e mitigação deve possuir serviço de atualização de assinaturas de ataques;
2. A CONTRATADA deve disponibilizar um Centro Operacional de Segurança no Brasil com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800 ou correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, durante a vigência da contratação do serviço;
3. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;
4. Em momentos de ataques DoS e DDoS, todo tráfego limpo deve ser reinjetado na infraestrutura da CONTRATANTE através de túneis GRE (Generic Routing Encapsulation), configurado entre a plataforma de DoS e DDoS da CONTRATADA e o CPE do CONTRATANTE;
5. As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta durante a vigência da contratação do serviço;
6. Em nenhum caso será aceito bloqueio de DoS e DDoS por ACLs configuradas em roteadores de bordas da CONTRATADA;
7. A CONTRATADA deve iniciar a mitigação de ataques em 60 minutos;
8. A CONTRATADA deverá disponibilizar relatório de monitoração de acompanhamento contra ataques DDoS;
9. O portal de gerenciamento deverá permitir acesso simultâneo a, pelo menos, um administrador de rede da CONTRATANTE;

14. Solução de Segurança Integrada

1. Todos os Itens do Lote 01 devem ser fornecida uma Solução Integrada de Segurança, compreende por:
    1. Características básicas
        1. Deverá ter hardware compatível com as características/necessidades do local a ser instalado especificadas no Anexo III;
        2. Deverá suportar número de conexões simultâneas compatível com as características/necessidades do local a ser instalado especificadas no Anexo III;
        3. Deverá suportar o throughput IPSec compatível com as características/necessidades do local a ser instalado especificadas no Anexo III;

14. Deverá ter quantidade de interfaces de rede compatíveis com as características/necessidades do local a ser instalado especificadas no Anexo III.

14. Funcionalidades de Firewall:

1. Permitir controle de acesso à internet por endereço IP de origem e destino, subrede e vlan;
2. Permitir a criação de VLANS no padrão IEEE 802.1q;
3. Deve possuir integração com Servidores de Autenticação RADIUS, LDAP e Microsoft Active Directory;
4. Suportar single-sign-on para Active Directory dos usuários da rede na solução de segurança;
5. Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

1. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para um, NAT64, NAT46, PAT;
2. Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
3. Possuir a funcionalidade de fazer tradução de endereços dinâmicos utilizando o IP da própria interface;
4. Suporte a roteamento estático e dinâmico RIP (v1 e v2), OSPF (v1 e v2) e BGPv4; 14.14.1.2.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede ou endereço IP de origem e destino;

14. Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay; 14.14.1.2.12. Deve implementar a funcionalidade de Stateful Firewall;

1. Deve permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;
2. Deve suportar PBR - Policy Based Routing;
3. Deve possuir conexão criptografada entre estação de gerência e solução de segurança tanto em interface gráfica quanto em CLI (linha de comando);
4. Permitir forwarding de camada 2 para protocolos não IP; 14.14.1.2.17. Deve suportar forwarding multicast, inclusive em modo bridge; 14.14.1.2.18. Suportar roteamento multicast PIM Sparse Mode ou Dense Mode;
5. Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;
6. Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
7. Possuir mecanismo de anti-spoofing de endereços IP;
8. Possuir a funcionalidade de balanceamento e contingência de links;
9. Permitir na solução de segurança a autenticação de usuários de rede em base local, servidor LDAP, RADIUS e TACACS;
10. Permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, horário, protocolo e aplicação;
11. Permitir a criação de endereços IPs virtuais;
12. Suportar balanceamento, ao menos, para os serviços HTTP, HTTPS, TCP e UDP; 14.14.1.2.27. Permitir balanceamento, ao menos, com os métodos hash do endereço IP de origem e Round Robin;
13. 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, quatro links;
14. Permitir persistência de sessão por cookie HTTP ou SSL session ID; 14.14.1.2.30. Permitir que seja mantido o IP de origem no cabeçalho HTTP;
15. Deve ter a capacidade de identificar, através de health checks, quais os links que estejam ativos;
16. Deve suportar a criação de instâncias virtuais na solução de segurança;

17. Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais da solução de segurança;
18. Deve permitir a criação de um administrador global que tenha acesso à todas as configurações das instâncias virtuais criadas na solução de segurança.
19. Funcionalidades de Prevenção de Intrusão, Controle de Ameaças e Antivírus: 14.14.1.3.1. Deve possuir base de assinaturas de IPS com pelo menos 3.000 ameaças conhecidas; 14.14.1.3.2. As assinaturas devem poder ser ativadas, desativadas ou habilitadas em modo de monitoração;
    1. Deve permitir ao IPS funcionar em modo transparente e/ou gateway;

1. Possuir tecnologia de detecção de ataques de IPS baseada em assinaturas que sejam atualizadas automaticamente;
2. Deve permitir a criação de padrões de ataque de IPS manualmente;
3. Deve possuir capacidade de agrupar assinaturas do IPS para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;
4. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
5. Deve prover notificação via Alarmes na console de administração e correio eletrônico para ataques detectados pelo IPS;
6. Deve possuir mecanismo de controle no IPS com as seguintes estratégias: pass, drop, reset;
7. Permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
8. Deve possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3 e FTP;
9. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.); 14.14.1.3.13. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

14. Possuir proteção contra conexões a servidores Botnet;

1. Funcionalidades de Filtro de conteúdo WEB:
    1. Deve possuir funcionalidade de filtro de conteúdo web integrado a solução de segurança;
    2. Deve possuir pelo menos 50 categorias ou sub-categorias para classificação de sites web;
    3. Deve possuir a funcionalidade de cota de tempo de utilização por categoria;
    4. Permitir a monitoração do tráfego internet por site e categoria web sem bloqueio de acesso aos usuários;

Permitir a re-classificação de sites web, tanto por URL quanto por endereço IP; 14.14.1.4.6. Deve permitir a criação de listas de URL específicas para serem bloqueadas ou liberadas;

1. Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;
2. Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
3. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP, endereço IP e sub-rede para a funcionalidade de filtro de conteúdo web; 14.14.1.4.10. Deve ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;

Permitir o bloqueio e continuação da navegação (possibilitando que o usuário acesse um site potencialmente bloqueado, informando o mesmo na tela de bloqueio, permitindo o usuário continuar acessando o site).

Controle de aplicação;

1. Reconhecer pelo menos 1.700 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;

1. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
3. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
4. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-a apenas pelo comportamento de tráfego da mesma;
5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados para a funcionalidade de controle de aplicações;
6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory para a funcionalidade de controle de aplicações;
7. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory para a funcionalidade de controle de aplicações;
8. Deve permitir criação de padrões de aplicação manualmente.
9. Funcionalidade de VPN;
    1. Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
    2. Suporte a certificados PKI X.509 para construção de VPNs;

Deve possuir suporte a VPNs IPSec site-to-site e client-to-site;

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

Deve permitir a arquitetura de vpn IPSec hub and spoke.

1. Funcionalidades de Gerência e Relatoria:
    1. A solução de gerência e relatoria deverá gerenciar, atualizar, configurar, monitorar e extrair dados para construção de relatórios de todos os equipamentos que compõem a Solução Integrada de Segurança que compõe os Lote de 1 a 42, nas quantidades mínimas informadas na Tabela 9 (Estimativa de Equipamentos e Serviços);
    2. A solução poderá ser entregue em forma de appliance ou máquina virtual, sendo que no caso de máquina virtual, toda a infra-estrutura necessária (servidores físicos, sistemas operacionais e softwares licenciados) deverá ser entregue em conjunto com a solução, de forma que suporte toda as funcionalidades e performance solicitadas neste Termo de Referência;
    3. Possuir interface gráfica de usuário (GUI) via HTTPS para fazer administração das políticas de segurança e que forme parte da arquitetura nativa da solução, por segurança, ou ainda, a solução pode ter interface proprietária, desde que a mesma seja fornecida com todos os componentes de hardware e software necessários;
    4. Possuir interface baseada em linha de comando para administração da solução de gerência;
    5. Comunicação cifrada e autenticada com usuário e senha na solução de gerência, tanto como para a interface gráfica de usuário como a console de administração de linha de comandos (SSH);
    6. Permitir a distribuição de políticas de segurança simultaneamente à distintos equipamentos de VPN e Firewall;

Possuir na solução de gerência perfis administrativos com capacidade de criar ao menos 2 (dois) perfis para administração e monitoração da Solução de Segurança e Wi- fi;

Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;

1. Deve ser capaz de atualizar remotamente a Solução Integrada de Segurança a partir de um ponto centralizado, sem intervenção local;
2. Possuir notificação via e-mail de eventos de gerência;
3. A gerência deve suportar log remoto no formato syslog;

1. A solução de gerência deve ser capaz de receber logs de vários dispositivos simultaneamente;
2. Permitir realização de backup e restauração dos dados do sistema de gerência;
3. Deve permitir habilitar e desabilitar, para cada interface de rede da solução de gerência, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;
4. Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;
5. A solução de gerência deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização;
6. Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas as mesmas somente sejam aplicadas após aprovação de outro administrador;
7. Deve permitir autenticação dos administradores da solução de gerência em servidor RADIUS e LDAP externo;
8. Deve permitir criar perfis diferenciados de leitura e escrita para os administradores da solução de gerência;
9. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;
10. Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência;
11. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como licenças, horário do sistema e firmware;
12. Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos;

Permitir visualizar de forma centralizada as licenças dos dispositivos gerenciados;

Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

1. Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;
2. Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência;
3. Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos;
4. Permitir criar políticas IPv4 e IPv6 a partir da solução de gerência;
5. As políticas aplicadas pela solução de gerência devem permitir configurar parâmetros de Endereços de origem e destino, Grupos, Usuários, interfaces de origem e destino, protocolo, ação, NAT, Log, autenticação e traffic shaping;
6. Permitir criar regras anti DoS de forma centralizada;
7. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;
8. Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia;
9. Deve permitir operar em alta disponibilidade (HA) sincronizando as configurações, objetos e políticas entre as estações de gerência;

10. Possuir interface gráfica de usuário (GUI) via HTTPS na solução de relatórios que forme parte da arquitetura nativa da solução, por segurança, ou ainda, a solução pode ter interface proprietária, desde que a mesma seja fornecida com todos os componentes de hardware e software necessários;

1. Possuir interface baseada em linha de comando para administração da solução de relatórios;
2. Comunicação cifrada e autenticada com usuário e senha na solução de relatórios, tanto como para a interface gráfica de usuário como a console de administração de linha de comandos (SSH);
3. Possuir perfis administrativos na solução de relatórios com capacidade de criar ao menos 2 (dois) perfis para administração e monitoração;
4. Suportar SNMP versão 2 e versão 3 na solução de relatórios;
5. Deve permitir virtualizar a solução de relatórios, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;
6. Deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização da solução de relatórios;
7. Deve permitir habilitar e desabilitar, para cada interface de rede da solução de relatórios, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;
8. Deve permitir autenticação dos administradores da solução de relatórios em servidor RADIUS e LDAP externo;
9. Deve permitir criar perfis diferenciados de leitura e escrita para os administradores da solução de relatórios;
10. Possuir "wizard" na solução de relatórios para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;
11. Possuir indicação de quantidade de logs enviadas por um dispositivo;
12. Deve possuir mecanismo de remoção automática de arquivos de log antigos na solução de relatórios;
13. Deve possuir mecanismo de envio automático de logs a um servidor FTP externo à solução;
14. Deve possuir relatórios pré definidos na solução de relatórios;
15. Deve permitir clonar e posteriormente editar relatórios existentes;
16. Deve permitir criar capas personalizadas para os relatórios;
17. Deve permitir importar e exportar relatórios;

Deve permitir criar gráficos dos tipos barra, linha e tabelas para inserção nos relatórios;

Deve possibilitar clonar gráficos existentes de relatórios;

1. Deve permitir criar consultas SQL ou equivalente personalizadas para uso nos gráficos e tabelas dos relatórios;
2. Permitir criar relatórios nos formatos HTML, PDF, XML e CSV;
3. Permitir o envio automático dos relatórios criados por email;

Permitir definir individualmente para cada relatório os emails que o receberão;

Permitir o envio automático dos relatórios criados à um servidor FTP ou SFTP externo à solução;

1. Permitir criação de relatórios no idioma Português;
2. Permitir programar dia e horário para a geração e envio automático dos relatórios;
3. Permitir a definição de filtros nos relatórios;
4. Permitir definir o layout do relatório, inserir textos e imagens, incluir gráficos, definir fontes, quebras de páginas, cores, alinhamento, entre outros;
5. Deve permitir definir alertas via email, syslog e snmp traps, baseados em eventos tais como ocorrência de determinado log, severidade de log, entre outros;

6. A solução de relatórios deve possuir dashboard gráfico, em tempo real, que indique dos dispositivos gerenciados quais as ocorrências de ameaças, ataques, origens, destinos, países, aplicações, websites, serviços e usuários;
7. A solução de relatórios deve possuir gráfico em tempo real indicando qual o consumo de disco e taxa de geração de logs dos dispositivos gerenciados;

1. Deve permitir visualizar de forma centralizada os logs detalhados recebidos por um determinado dispositivo e/ou por todos os dispositivos, incluindo capacidade de aplicação de filtros nas pesquisas destes logs;
2. Deve possibilitar efetuar download dos arquivos de logs recebidos;
3. Indicar na GUI da solução de relatórios informações do sistema de logs tais como licenças, uso de CPU, memória, disco, taxa de recebimento de logs por segundo, total de logs diários recebidos, alertas gerados entre outros;
4. Suportar capacidade mínima de logs diários de 500 Gbytes;
5. Suportar capacidade mínima de processamento de 80.000 log's por segundo.
6. Funcionalidade de Autenticação de Segurança;
    1. A solução deve efetuar autenticação para a gerência de identidade dos usuários da rede, ajudando a simplificar a administração dos mesmos sendo um ponto central de controle de autenticação, onde múltiplos métodos de autenticação possam ser consolidados;
    2. Deve possuir suporte a autenticação de dois fatores em pelo menos dois tipos diferentes de tokens, sendo o primeiro físico (token), e o segundo lógico como software para dispositivos móveis, e-mail ou SMS, permitindo que seja dada a escolha de qual dos tipos utilizar para cada usuário;
    3. A solução deve permitir que se defina um perfil de complexidade mínimo para as senhas de todos os usuários cadastrados na base de dados local, possibilitando a definição de número mínimo de letras minúsculas, letras maiúsculas, caracteres numéricos, caracteres especiais e etc.
    4. A solução deve suportar a criação de usuários em base local, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;
    5. A solução deve permitir a criação em massa de usuários na base de dados local através da importação de lista de usuários a serem criados contida em arquivos externos;
    6. A solução deve permitir a criação de novos usuários na base de dados local e que o criador/administrador possa definir uma senha no momento de criação do mesmo;
    7. Deve continuar permitindo a autenticação de dois fatores em clientes windows mesmo com a máquina offline;
    8. A solução deve funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
    9. A solução deve suportar a integração com servidor RADIUS remoto;
    10. A solução deve possuir um servidor LDAP interno que permita ser configurado de forma hierárquica, para a correta administração por grupos ou unidades organizacionais dos usuários locais;
    11. A solução deve suportar a integração com servidor LDAP remoto (como Microsoft Active Directory);
    12. A solução deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autentiquem através de um rápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone;
    13. A solução deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+;
    14. Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo uma relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider - SP);

15. A solução deve suportar nativamente (sem redirecionamentos) a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X;
16. Suportar os seguintes métodos 802.1X EAP: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS e EAP-GTC;
17. Suportar interoperabilidade com equipamentos de acesso (switches) de outros fabricantes, para autenticação de portas junto a solução, através dos padrões 802.1X;
18. A solução deve atuar como Autoridade Certificadora (CA);

1. Deve permitir a administração de certificados digitais, com emissão e revogação;
2. Deve permitir o uso de CA's confiáveis para validação de certificados emitidos por CA's externas;

Deve prover repositório para autenticação de VPN Site-to-Site através de Certificados;

Deve suportar SCEP server (Simple Certificate Enrollment Protocol), permitindo a assinatura de requisições de certificados digitais (CSR) automaticamente ou com interação do administrador;

1. Deve ser capaz de importar outros certificados de CA's assim como a lista de certificados revogados;
2. Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade se SSO, onde a autenticação automática/transparente via SSO para os serviços necessários é baseada na autenticação prévia feita pelo usuário no domínio;
3. Deve suportar Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Indentity Providers - IDP's) de terceiros;
4. Deve suportar RSSO Accounting Proxy permitindo a recepção de pacotes radius de accouting, a modificação destes pacotes e o encaminhamento dos mesmos para vários outros pontos.
5. Solução de Gerenciamento e Distribuição Sem Fio;
    1. A solução deve ser capaz de gerenciar centralizadamente pontos de acesso da solução ofertada;
    2. Prover endereçamento IP automático para os clientes wireless através de serviço de servidor DHCP por SSID;
    3. Suporte a monitoração e supressão de ponto de acesso indevido;
    4. Prover autenticação para a rede wireless através de bases externas como LDAP, RADIUS ou TACACS+;
    5. Deverá permitir a visualização dos clientes conectados;
    6. Deverá prover suporte a Fast Roaming;
    7. Possuir Captive Portal por SSID;
    8. Permitir configurar o bloqueio de tráfego entre SSIDs;
    9. Deverá suportar Wi-Fi Protected Access (WPA) e WPA2 por SSID, utilizando-se de AES e/ou TKIP;
    10. Deverá suportar 802.1x através de RADIUS;
    11. Permitir configurar parâmetros de rádio como: banda e canal;
    12. Possuir método de descoberta de novos pontos de acesso baseados em Broadcast ou Multicast;
    13. Possuir lista contendo pontos de acesso aceitos e pontos de acesso indevidos (Rogue);
    14. Possuir WIDS com ao menos os seguintes perfis: Asleap Attack, Association/Authentication Frame Flooding, Broadcasting De-authentication, Spoofed De- authentication, Wireless Bridge;
    15. A controladora deverá oferecer firewall integrado ou integração com sistema de firewall, baseado em identidade do usuário;
    16. Possibilitar definir número de clientes por SSID;
    17. Possuir mecanismo de criação automática de usuários visitantes e senhas auto-geradas e/ou manual, que possam ser enviadas por email ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

18. A comunicação entre o ponto de acesso e a controladora wi-fi deve poder ser efetuada de forma criptografada;
19. Deve possuir mecanismo de ajuste de potência do sinal de forma a reduzir interferência entre canais entre dois pontos de acesso gerenciados;

1. Deve permitir a identificação de pontos de acesso com firmware desatualizado e efetuar o upgrade via interface gráfica.
2. A CONTRATADA deverá ativar 10 (dez) equipamentos (pontos de acesso) por Campus e gerenciados pela solução integrada;
3. A CONTRATADA disponibilizará central de atendimento especializado e personalizado para comunicação de falhas e inoperâncias do circuito/porta de acesso. O atendimento será prestado através de ligação telefônica gratuita via 0800, disponível 24 horas por dia, sete dias por semana;
4. Solução de Videoconferência
5. Solução de Videoconferência para Salas de reunião, desktops e dispositivos móveis, que deverá possuir, no mínimo, os componentes descritos a seguir, de modo a atender aos requisitos e funcionalidades do Serviço de Videoconferência previstos nesta especificação:
    1. Solução deve ser fornecida como serviço de SAAS (Serviço em nuvem);
    2. Reuniões Simultâneas (licença de sala virtual): As licenças deverão permitir a criação e o gerenciamento de no mínimo 10 (dez) salas virtuais disponíveis em tempo integral aos usuários, tanto organizadores das reuniões como os usuários convidados, dentro e fora da CONTRATANTE.
    3. Deve permitir compartilhamento de documento, aplicativo e tela do computador;
    4. Compatível com as plataformas: Microsoft Windows, Linux, Android e iOS;
    5. Deve permitir a gravação e acesso às reuniões gravadas;
    6. Deve permitir a personalização da URL;
    7. .Serviços de Suporte, Manutenção, Garantia e Gerenciamento e Prazos:
6. Serviço de instalação, configuração e manutenção de todos os equipamentos para o correto funcionamento dos links de comunicação nos termos deste Termo de Referência;
7. A manutenção visa manter em perfeito estado de operação os serviços e equipamentos fornecidos em atendimento ao objeto, deste modo a CONTRATADA deve cumprir os seguintes procedimentos:
    1. Do hardware: desinstalação, reconfiguração ou reinstalação decorrentes de falhas no hardware, fornecimento de peças de reposição, substituição de hardware, atualização da versão de drivers, firmwares e software básico, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados.
    2. Do software (aplicativos e sistema operacional): desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;
    3. Quanto às atualizações pertinentes aos softwares, entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado.
8. A CONTRATADA deverá prover um serviço de gerência proativa de rede que atue em seu backbone, para fins de detecção, encaminhamento e solução de problemas, sendo que o CBMRR poderá ter acesso de leitura aos roteadores da rede.
9. A gerência de rede da CONTRATADA deverá estar disponível 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, sem interrupção. Visando a manutenção da disponibilidade dos serviços fora do horário comercial, momento em que ocorrem vários eventos e trabalhos específicos.
10. Será função da gerência de rede da CONTRATADA realizar ações pró-ativas que permitam garantir os níveis de serviço contratados relativos ao retardo, disponibilidade e desempenho da rede contratada.

1. Na ocorrência de qualquer falha nos acessos contratados, a gerência de rede da CONTRATADA deverá iniciar o processo de recuperação de falhas fazendo o registro da ocorrência e o posterior acompanhamento de sua solução.
2. Deverão ser disponibilizadas no portal web informações de desempenho do serviço de rede dos equipamentos CPE, na forma textual e/ou gráfica, obtidas através do uso de SNMP, ICMP ou outro protocolo de controle de rede, incluindo:
    1. Identificação de cada roteador;
    2. Descarte de pacotes e quadros;
    3. Taxa média de ocupação do acesso, por hora;
    4. Latência entre cada uma das localidades contratadas;
    5. Taxa de erro máxima por acesso.
3. As informações de desempenho deverão ser disponibilizadas na forma de gráficos gerados ao longo do tempo, em intervalos não superiores a 5 (cinco) minutos e disponibilizados em intervalos não superiores a 30 (trinta) minutos, mostrando os valores máximos e médios de desempenho de todos os acessos contratados e do Backbone da CONTRATADA.
4. Manutenção Corretiva com tempo de resposta previsto no Nível Mínimo de Serviço. Entende-se por tempo de resposta como o prazo máximo para o deslocamento de técnico da contratada até o endereço associado à reclamação de suporte (se necessário o deslocamento) e, por tempo de solução como o prazo máximo para a resolução do problema em questão;
5. A CONTRATADA deverá quando solicitado pelo CONTRATANTE, apresentar relatório com informações de disponibilidade, utilização, tráfego (entrante e sainte) e falha do link;
6. O prazo de entrega do serviço será conforme os Níveis de Serviço Mínimos Exigidos contemplados, em dias corridos, a partir da solicitação formal do órgão CONTRATANTE. A entrega será considerada concluída, para efeito de cobrança quando:
    1. Execução do primeiro acesso ao sistema de monitoração de tráfego, com visualização de dados reais;
    2. Testes de conectividades que atenda os parâmetros técnicos estabelecidos nos Níveis de Serviços Exigidos contemplados;
    3. Os testes de conectividades serão realizados pelas equipes técnicas da CONTRATANTE e da CONTRATADA, sendo admitida a participação remota das equipes envolvidas;
7. Após os requisitos acima atendidos, deverá ser formalizada em documento a data efetiva de ativação do link para efeito de cobrança de fatura;
8. Caso a entrega do acesso e a disponibilização do serviço não forem realizados nos prazos especificados, a CONTRATANTE aplicará multa conforme disposto no contrato;
9. Interrupções programadas, para manutenção preventiva ou atualização dos recursos técnicos utilizados na prestação do serviço, deverão seguir os parâmetros dos Níveis Mínimos de Serviço;
10. Para cada problema constatado de indisponibilidade não programada do link de comunicação com a Internet, a CONTRATADA deverá apresentar relatório técnico apresentando as causas do problema, solução adotada e medidas para evitar a reincidência;
11. No caso de inoperância reincidente num período de até 3 (três) horas, contados a partir do restabelecimento do serviço, considerar-se-á como tempo de indisponibilidade do circuito, o tempo transcorrido desde o início da primeira inoperância até o final da última inoperância, quando o circuito estiver totalmente operacional. Neste caso, acarretará aplicação de multa conforme disposto no contrato;
12. A CONTRATANTE poderá mediante comunicado formal, com pelo menos 30 (trinta) dias de antecedência, solicitar o cancelamento de qualquer um dos circuitos contratados;
13. A CONTRATADA deverá disponibilizar para a CONTRATANTE acesso ao Sistema Web de Monitoramento de disponibilidade, utilização e falha do link. O sistema deve permitir a geração de relatórios periódicos de desempenho, disponibilidade e falhas do link para auxílio no gerenciamento e nos atestes de fatura. O sistema deve possuir informações gráficas.

14.16. Níveis Mínimos de Serviço Exigidos (NMS)

1. O contratante avaliará os serviços executados em cada ordem de serviço e em cada chamado técnico por meio da utilização de Indicadores de Nível de Serviço Exigidos (INMS), que são critérios objetivos e mensuráveis estabelecidos entre o contratante e a contratada, com a finalidade de aferir e avaliar aspectos de tempo e qualidade relacionados aos serviços contratados.
2. O desconto não será aplicado se o CONTRATANTE der causa à variação do INMS, por exemplo, indisponibilidade da área demandante, por exemplo, falta de energia, etc.
3. Os descontos referentes aos indicadores descritos são cumulativos, sendo que seu somatório não poderá ultrapassar 20% do valor do link contratado. A partir de 20% de desconto, o CONTRATANTE se reserva o direito de caracterizar o descumprimento parcial das obrigações assumidas.
4. Os indicadores serão medidos desde o início da execução contratual, nas periodicidades definidas, e a CONTRATADA será informada dos resultados, para que providencie as eventuais adequações que se fizerem necessárias na dinâmica da prestação dos serviços.

A apuração da disponibilidade deve ser calculada da seguinte forma:

D% = [(T1-T2) / T1] * 100, onde:

D = Disponibilidade

T1 = Total de minutos do mês

T2 = Total de minutos com interrupção de serviços

Eventos de falhas excluídos do cálculo da disponibilidade:

1. Falha de qualquer componente que não possa ser corrigida por impossibilidade de acesso pela(s) CONTRATADA(s) a equipamentos que estejam no ambiente e instalações sob coordenação de uma unidade da CONTRATANTE;
2. Falha decorrente de problemas de infraestrutura provida no local e de responsabilidade de uma unidade da CONTRATANTE para os serviços prestados pela(s) CONTRATADA(s);
3. Interrupções programadas e avisadas com a devida antecedência, conforme estabelecido em contrato;
4. Horário de funcionamento da unidade na localidade para atendimento a ocorrências de Segunda a Domingo, 24x7, para os links contratados ou de acordo com o horário estabelecido nos Níveis Mínimos de Serviço contemplados;
5. Tempo máximo de latência do equipamento na localidade, unidade remota, e o roteador de borda de saída da CONTRATADA para a Internet instalada na rede da CONTRATADA, conforme discriminado nos Níveis Mínimos de Serviço contemplados;
6. Tempo máximo de solução para resolução de problemas de indisponibilidade, conforme discriminado nos Níveis Mínimos de Serviço contemplados;
7. A CONTRATADA deve prever o fornecimento, instalação, configuração e manutenção de todos os equipamentos de telecomunicação necessários para a utilização de cada acesso à Internet, incluindo roteadores ou quaisquer outros equipamentos que se façam necessários atendendo as velocidades contratadas e os Níveis Mínimos de Serviço contemplados;
8. Os dispositivos de rede utilizados em cada ponto remoto contemplado deverão possuir e ser configurados para a utilização de gerenciamento via SNMP;
9. A configuração de gerenciamento via SNMP deverá ser definida pela equipe técnica do CBMRR e homologada entre a CONTRATADA e a equipe técnica do órgão;
10. Todo o plano de endereçamento IP a ser utilizado na configuração dos equipamentos de telecomunicações deverá ser definido pela equipe técnica da empresa CONTRATADA em conjunto com a equipe técnica da CONTRATANTE;

1. No fornecimento do serviço de acesso à rede mundial de computadores – Internet, a CONTRATADA, deve prever utilização do serviço de tradução de endereço (NAT) no equipamento de acesso disponibilizado em cada unidade remota.

14.17. Dinâmica da Execução

1. Ordens de Serviço (OS)

1. A Ordem de Serviço é o instrumento formal pelo qual o CONTRATANTE encaminha a demanda de serviço para a CONTRATADA.
2. A Ordem de Serviço será aplicada para os casos de Ativação de Circuito Novo, Alteração de Endereço de Circuito e Desligamento de Circuito.
3. As Ordens de Serviço deverão conter as informações mínimas necessárias à execução dos serviços demandados à CONTRATADA, conforme estabelecido nos tipos de modelos de execução descritos a seguir.
4. As Ordens de Serviço e os Chamados Técnicos, serão emitidas, acompanhadas e revisadas pelo CONTRATANTE.
5. O prazo de início e término da execução dos serviços será registrado na própria Ordem de Serviço.
6. Os modelos de Ordem de Serviço poderão, a critério do CONTRATANTE, ser alterados a qualquer momento para atender as necessidades do serviço, devendo, contudo, manter as informações mínimas necessárias para sua execução.
7. Todos os serviços deverão ser elaborados por profissionais devidamente qualificados.
8. No caso de existirem orientações específicas para a execução do serviço contidas na Ordem de Serviço, prevalecerá o descrito nesse documento, ainda que diverso do estabelecido nos padrões e processos de trabalho do CONTRATANTE, no que diz respeito aos insumos, produtos a serem gerados ou atividades a serem executadas na Ordem de Serviço.
9. Para as Ordens de Serviço em que a CONTRATADA tiver documentado o detalhamento de atendimento, devidamente aprovado pelo CONTRATANTE, a execução dos serviços deverá obedecer estritamente este delineamento:
    1. A CONTRATADA deverá propor alterações na forma de execução ao CONTRATANTE, na hipótese de:
        1. Identificar riscos ou problemas na execução da Ordem de Serviço, seguindo os padrões e processos de trabalho do CONTRATANTE ou, se for o caso, no seu detalhamento de atendimento ou
        2. Identificar forma mais adequada de solução para a Ordem de Serviço específica;
        3. A CONTRATADA deverá, tempestivamente, se ajustar às alterações nos padrões e processos de trabalho que venham a ser implementados pelo CONTRATANTE.
10. Durante toda a execução da Ordem de Serviço, a CONTRATADA deverá manter a resolução da demanda adequadamente documentada em sistema próprio, no qual o fiscal técnico deverá ter acesso para acompanhamento. Excepcionalmente, o CONTRATANTE poderá, a seu critério, aceitar o controle manual das demandas por meio de outras formas eletrônicas.
11. Não obstante ser a CONTRATADA a única e exclusiva responsável pela execução de todos os serviços, o CONTRATANTE reserva-se o direito de, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização.

.Chamados Técnicos

1. Para a abertura de chamados técnicos de reparo ou de qualquer outra ação, será utilizada a metodologia descrita no item 14.16.1 e demais itens relativos ao sistema de abertura de chamados da CONTRATADA conforme descrito neste Contrato.

CLÁUSULA DÉCIMA QUINTA – DO SIGILO, PROPRIEDADE DAS INFORMAÇÕES, DIREITO PATRIMONIAL E PROPRIEDADE INTELECTUAL

15. A CONTRATADA cederá ao CONTRATANTE a propriedade intelectual em caráter definitivo dos resultados produzidos em consequência desta licitação, entendendo-se por resultados quaisquer estudos, relatórios, descrições técnicas, dados, esquemas, plantas, desenhos, diagramas e documentação didática em papel ou em mídia eletrônica. Assim todas as informações obtidas e/ou produzidas decorrentes da

contratação execução das atividades são de propriedades da CONTRATANTE e/ou órgãos vinculados a essa Ata de Registro de Preços.

15. A CONTRATADA e todos os funcionários envolvidos no processo de execução das atividades deverão manter sigilo absoluto sobre quaisquer informações da CONTRATANTE e órgãos vinculados a essa Ata de Registro de Preços.

15. A CONTRATADA, através de seu representante, deverá assinar o Acordo de Confidencialidade de Informação e dar ciência do mesmo a toda sua equipe de profissionais que participarão da execução do contrato.

CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS

16.1. Os casos omissos relativos à execução deste contrato administrativo serão resolvidos pelas partes, com a estrita observância das disposições contidas nos termos da Lei Federal 10.520/02, Lei Federal nº 8.666/93 Lei Estadual nº 7.696/02 e Decreto Estadual nº 840/17 e alterações posteriores, bem como as demais legislações complementares aplicáveis a espécie.

CLÁUSULA DÉCIMA SÉTIMA – DA CLÁUSULA ANTICORRUPÇÃO

17.1. Para a execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios de qualquer espécie, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma a ele não relacionada, o que deve ser observado, ainda, pelos prepostos e colaboradores, artigo 138, do Decreto Estadual nº 840/2017.

CLÁUSULA DÉCIMA OITAVA – DAS DISPOSIÇÕES GERAIS

18. Este Contrato deverá ser executado fielmente pelas partes de acordo com as cláusulas avençadas e as normas previstas na Lei n° 8.666/1993, respondendo elas pelas consequências de sua inexecução total ou parcial.

18. A declaração de nulidade deste Contrato opera retroativamente, impedindo efeitos jurídicos que nele, ordinariamente, deverá produzir, além de desconstituir os que porventura já tenha produzido.

18. A declaração de nulidade não exonera o CONTRATANTE do dever de indenizar a CONTRATADA pelo que esta houver executado, e por outros prejuízos regularmente comprovados contanto que não lhe seja imputável, promovendo a responsabilidade de quem lhe deu causa.

18. As supressões poderão ultrapassar o limite acima estabelecido, havendo acordo entre as partes;

18. O Contratante poderá revogar este Contrato, por razões de interesse público decorrente de fato superveniente, devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-lo por ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado;

    1. A declaração de nulidade deste Contrato opera retroativamente, impedindo efeitos jurídicos que nele, ordinariamente, deverá produzir, além de desconstituir os que porventura já tenha produzido;

    2. A nulidade não exonera o Contratante do dever de indenizar o Contratado pelo que este houver executado até a data em que ela for declarada e por outros prejuízos regularmente comprovados, contanto que não lhe seja imputável, promovendo a responsabilidade de quem lhe deu causa;

    3. Não será permitido à subcontratação parcial ou total do objeto do Contrato, quando se verificarem as hipóteses de impossibilidade técnica da realização do serviço solicitado a empresa contratada, desde que esta se responsabilize pelo seu fornecimento/serviço e consequente garantia.

18.5 Incumbirá ao Contratante, providenciar a publicação do extrato deste contrato, em conformidade com o disposto no art. 61, Parágrafo Único, da Lei nº 8.666/1993.

CLÁUSULA DÉCIMA NOVA – DA LEGISLAÇÃO APLICADA

19. – Lei 8.666/93 e alterações – normas para Licitação;

19. – Lei 10.520/2002 – Institui o Pregão;
19. – Decreto Estadual nº 840/2017 e alterações – Regra para Aquisição;
19. - Decreto Estadual nº 8.199/2006 e Decreto Estadual nº 011/2015 – Critério de Pagamento;
19. – Decreto Federal nº 7.892/2013 – Regulamenta RP.

CLÁUSULA VIGÉSIMA – DO FORO

20.1. Fica eleito o foro da cidade de Cáceres, Estado de Mato Grosso, como competente para dirimir quaisquer dúvidas ou questões decorrentes da execução deste contrato.

E por estarem de acordo, as partes firmam o presente contrato, em 03 (quatro) vias de igual teor e forma para um só efeito legal, ficando uma via arquivada na sede da contratante, na forma do art. 60 da Lei 8 666 de 21/06/93.

CONTRATANTE:
Jean Claudio de Souza Hermógenes - CEL QOCBM Comandante Geral do CBMRR
CONTRATADA:
Raul Luiz Martins Peregrino Executivo de Negócios OI SA Brasil Dias de Souza Executivo de Negócios OI S/A

Nome do Responsável REPRESENTANTE LEGAL:

TESTEMUNHAS:

Nome: Nome:

C.I.: C.I.:

Documento assinado eletronicamente por **Brasil Dias de Souza**, **Usuário Externo**, em 01/09/2020, às 17:21, conforme Art. 5º, XIII, "b", do Decreto Nº 27.971-E/2019.

Documento assinado eletronicamente por **Jean Cláudio de Souza Hermógenes**, **Comandante Geral**, em 03/09/2020, às 11:33, conforme Art. 5º, XIII, "b", do Decreto Nº 27.971-E/2019.

Documento assinado eletronicamente por **Raul Luiz Martins Peregrino**, **Usuário Externo**, em 04/09/2020, às 11:48, conforme Art. 5º, XIII, "b", do Decreto Nº 27.971-E/2019.

A autenticidade do documento pode ser conferida no endereço https://sei.rr.gov.br/autenticar informando o código verificador **0361133** e o código CRC **558586F8**.