MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO
Escritório de Projetos e Contratações da DTI.
Setor de Autarquias Sul Quadra 1 Bloco A, Edifício Darcy Ribeiro - Bairro Asa sul, Brasília/DF, CEP 70070-905
Telefone: - - www.cgu.gov.br

TERMO DE REFERÊNCIA PROCESSO DE CONTRATAÇÃO

1. DO OBJETO

1.1. Contratação de provimento de serviço de comunicação que compõe a Rede WAN MPLS (Multiprotocol Label Switching) da CGU, incluindo as conexões com a Internet na sede e nas unidades regionais, por meio de Sistema de Registro de Preços, conforme definição constante deste termo de referência e anexos.

2. DA JUSTIFICATIVA

2.1. Este termo visa contratação de empresa para fornecimento da Rede WAN MPLS da CGU tendo em vista a previsão de finalização do contrato vigente;

2.2. A Rede é responsável pela interconexão entre as unidades regionais da CGU à sede usando um meio seguro, confiável e estável. A necessidade desta infraestrutura se justifica pela necessidade das unidades regionais acessarem serviços de TI hospedados na Sede tais como: Sistemas Internos (Ativa, IntraCGU, SEI, SGI dentre outros), Serviços de Ti (Correio Eletrônico, Skype for Business, BDI, Internet, videoconferência). Essa rede é necessária para garantir este acesso nos níveis mínimos de qualidades;

2.3. Adicionalmente, pretende-se ampliar o serviço atualmente ofertado incluindo nova alternativa de interconexão das regionais com a Internet. Estas conexões locais resultarão em serviço de acesso à Internet de melhor qualidade e ampliará a resiliência do sistema visto que constituirá uma segunda rota (contingência) de acesso aos serviços corporativos. Para isso, serão integrados a esta contratação os serviços de acesso à internet da Sede;

3. Destaca-se que a iniciativa está prevista no Plano Diretor de Tecnologia da Informação - PDTI 2017-2018 deste Ministério, no item 8.2 Sustentação dos serviços de TI oferecidos à Casa:

3.1. Prestação dos serviços de comunicação de dados/voz/imagem – rede WAN;

3.2. Serviço de acesso IP permanente.

4. DO ENQUADRAMENTO DOS SERVIÇOS

4.1. O objeto da presente contratação pode ser objetivamente especificado por meio de padrões usuais de mercado. Desta forma, entendemos que o objeto pode ser classificado como bem/serviço comum, para fins do disposto no parágrafo único, art 1º da Lei 10.520, de 17 de julho de 2002, podendo, portanto, ser adquiridos por meio de processo licitatório na modalidade pregão;

4.2. Será permitida a participação de empresas em consórcio, observado o disposto no art. 33 da lei 8.666/93, desde que pertençam ao mesmo grupo econômico;

4.2.1. A permissão objetiva viabilizar a prestação eficiente de serviços previstos que não são propriamente de telecomunicações;

4.2.2. A restrição a empresas de mesmo grupo econômico decorre da necessidade de que esses serviços sejam prestados de forma eficaz e de forma totalmente integrada com todo o sistema a ser contratado.

4.3. Uma vez que os itens contratados suportam serviços que apoiam a execução das atividades finalísticas do Ministério, de forma a garantir o atingimento de sua missão institucional, o serviço de comunicação que compõe a Rede WAN MPLS (Multiprotocol Label Switching) da CGU, incluindo as conexões com a Internet na sede e nas unidades regionais, possui caráter continuado;

4.4. A contratação será realizada por meio de Sistema de Registro de Preço, conforme inciso I e IV do Art.3° do Decreto 7.892/2013, uma vez caracterizada a necessidade de contratações frequentes e que, pela natureza do objeto, não foi possível definir previamente alguns quantitativos a serem demandados pela Administração;

4.4.1. Considerando tratar-se de implantação de infraestrutura de rede própria que visa atender unicamente a CGU que possui especificidades técnicas próprias, não será permitida a participação de outros órgãos e entidades da Administração Pública no SRP, bem como futuras adesões à Ata de Registro de Preços.

5. DOS QUANTITATIVOS

Lote	Item	Descrição	Qtde Registrada	Qtde Inicial	Unidade
1	1	Link MPLS - Regional Tipo 1 – AC	24	0	Mês
	2	Link MPLS - Regional Tipo 1 – AL	24	0	Mês
	3	Link MPLS - Regional Tipo 1 – AM	24	0	Mês
	4	Link MPLS - Regional Tipo 1 – AP	24	0	Mês
	5	Link MPLS - Regional Tipo 1 – ES	24	0	Mês
	6	Link MPLS - Regional Tipo 1 – MA	24	0	Mês
	7	Link MPLS - Regional Tipo 1 – MS	24	0	Mês
	8	Link MPLS - Regional Tipo 1 – MT	24	0	Mês
	9	Link MPLS - Regional Tipo 1 – PB	24	0	Mês
	10	Link MPLS - Regional Tipo 1 – PI	24	0	Mês
	11	Link MPLS - Regional Tipo 1 – RN	24	0	Mês
	12	Link MPLS - Regional Tipo 1 – RO	24	0	Mês
	13	Link MPLS - Regional Tipo 1 – RR	24	0	Mês

14	Link MPLS - Regional Tipo 1 – SC	24	0	Mês
15	Link MPLS - Regional Tipo 1 – SE	24	0	Mês
16	Link MPLS - Regional Tipo 1 – TO	24	0	Mês
17	Link MPLS - Regional Tipo 2 – BA	24	0	Mês
18	Link MPLS - Regional Tipo 2 – CE	24	0	Mês
19	Link MPLS - Regional Tipo 2 – GO	24	0	Mês
20	Link MPLS - Regional Tipo 2 – PA	24	0	Mês
21	Link MPLS - Regional Tipo 2 – PE	24	0	Mês
22	Link MPLS - Regional Tipo 2 – PR	24	0	Mês
23	Link MPLS - Regional Tipo 2 – RS	24	0	Mês
24	Link MPLS - Regional Tipo 3 – MG	24	0	Mês
25	Link MPLS - Regional Tipo 3 – RJ	24	0	Mês
26	Link MPLS - Regional Tipo 3 – SP	24	0	Mês
27	2 (dois) Links MPLS - Sede – DF	24	0	Mês
28	2 (dois) Roteadores MPLS – Sede	24	0	Mês
29	Link Internet - Regional Tipo 1 – AC	24	0	Mês
30	Link Internet - Regional Tipo 1 – AL	24	0	Mês
31	Link Internet - Regional Tipo 1 – AM	24	0	Mês
32	Link Internet - Regional Tipo 1 – AP	24	0	Mês
33	Link Internet - Regional Tipo 1 – ES	24	0	Mês
34	Link Internet - Regional Tipo 1 – MA	24	0	Mês
35	Link Internet - Regional Tipo 1 – MS	24	0	Mês
36	Link Internet - Regional Tipo 1 – MT	24	0	Mês
37	Link Internet - Regional Tipo 1 – PB	24	0	Mês
38	Link Internet - Regional Tipo 1 – PI	24	0	Mês
39	Link Internet - Regional Tipo 1 – RN	24	0	Mês
40	Link Internet - Regional Tipo 1 – RO	24	0	Mês
41	Link Internet - Regional Tipo 1 – RR	24	0	Mês
42	Link Internet - Regional Tipo 1 – SC	24	0	Mês
43	Link Internet - Regional Tipo 1 – SE	24	0	Mês
44	Link Internet - Regional Tipo 1 – TO	24	0	Mês
45	Link Internet - Regional Tipo 2 – BA	24	0	Mês
46	Link Internet - Regional Tipo 2 – CE	24	0	Mês
47	Link Internet - Regional Tipo 2 – GO	24	0	Mês
48	Link Internet - Regional Tipo 2 – PA	24	0	Mês

	49	Link Internet - Regional Tipo 2 – PE	24	0	Mês
	50	Link Internet - Regional Tipo 2 – PR	24	0	Mês
	51	Link Internet - Regional Tipo 2 – RS	24	0	Mês
	52	Link Internet - Regional Tipo 3 – MG	24	0	Mês
	53	Link Internet - Regional Tipo 3 – RJ	24	0	Mês
	54	Link Internet - Regional Tipo 3 – SP	24	0	Mês
	55	16 (dezesseis) Appliances de Firewall/Filtro de Conteúdo - Regionais Tipo 1	24	0	Mês
	56	7 (sete) Appliances de Firewall/Filtro de Conteúdo - Regionais Tipo 2	24	0	Mês
	57	3 (três) Appliances de Firewall/Filtro de Conteúdo - Regionais Tipo 3	24	0	Mês
	58	2 (dois) Appliances de Firewall/Filtro de Conteúdo – Sede	24	0	Mês
	59	Solução de Gerência dos e Appliances de Firewall/Filtro de Conteúdo	24	0	Mês
	60	Solução de Netflow	24	0	Mês
	61	Link Internet - Sede 1	24	0	Mês
	62	Roteador Internet - Sede 1	24	0	Mês
	63	Serviço de Mudança de Endereço	12	0	Serviço de mudança de Endereço
	64	Implantação solução - Lote 1	1	1	Implantação
	65	Repasse de Conhecimento - Solução Firewall/Filtro de Conteúdo	1	0	Turma
	66	Repasse de Conhecimento - Roteador Internet - Sede 1	1	0	Turma
2	67	Link Internet - Sede 2	24	0	Mês
	68	Roteador Internet - Sede 2	24	0	Mês
	69	Implantação Solução - Lote 2	1	1	Implantação
	70	Repasse de Conhecimento - Roteador Internet - Sede 2	1	0	Turma

Tabela 1 – Itens e quantitativos

5.1. Quanto ao agrupamento em lotes:

5.1.1. Os itens foram agrupados em dois lotes, tendo em vista a interdependência dos itens ao formarem soluções integradas de comunicação, respectivamente, o primeiro lote conformando o sistema Rede WAN MPLS e o segundo lote conformando o segundo Link de Internet da CGU. Sendo assim, os itens que compõem cada lote devem ser licitados de forma agrupadas e serem entregues por empresa única de forma viabilizar o funcionamento das soluções;

5.1.2. Conforme disciplinado no edital vinculado a este Termo de Referência, a mesma empresa não poderá lograr vencedora dos dois lotes;

5.1.2.1. Caso uma licitante seja vencedora dos dois lotes, ela deverá optar por qual lote será classificada.

5.1.3. Esta restrição decorre dos seguintes elementos:

5.1.3.1. Visa garantir mais segurança à CONTRATANTE por meio da redundância de sistema autônomo e de provedores de trânsito. Assim, torna-se impedido o compartilhamento de qualquer tipo de infraestrutura e provedores de trânsito, com o objetivo de evitar indisponibilidade simultânea das duas conexões de internet da sede da CGU. As conexões de internet da sede da CGU são especialmente críticas porque, além de proverem conectividade para cerca de 1500 colaboradores, os links também irão permitir acesso a diversos serviços que a CGU disponibiliza pela internet, como correio eletrônico e diversos sistemas internos. Esses serviços são acessados por colaboradores em trabalho externo bem como por aqueles que estiverem em regime de teletrabalho;

5.1.3.2. Devido à complexidade técnica da solução, entende-se que a gestão dos diversos serviços que compõem cada um dos lotes dever ser realizada por uma única empresa. Não raro, soluções técnicas interdependentes que são geridas por diferentes empresas apresentam conflitos de responsabilidade na ocorrência de um problema técnico em que nenhuma das empresas assume a responsabilidade do problema e a solução fica indisponível até que o fiscal técnico defina de quem é a responsabilidade em um caso concreto;

5.1.3.3. Os itens relativos aos links MPLS e internet das unidades regionais bem como os CPEs e Firewalls/Filtros de conteúdo formarão uma única solução com grande relação de interdependência. Essa solução (equipamentos e links operando em conjunto) será responsável por garantir a arquitetura de alta disponibilidade da sede da CGU e de suas unidades regionais, incluindo o balanceamento de tráfego conforme o perfil.

5.1.4. Ainda, todos os links internet das regionais e o PE que atenderá o link internet (Item 61) devem necessariamente pertencer às ASes do mesmo grupo econômico para que a latência do túnel VPN seja reduzida. Por esse motivo o referido item deve ser licitado em conjunto com os demais itens do lote 1;

5.2. Quanto às unidades iniciais:

5.2.1. Os itens 64 e 69 possuem, cada, quantitativo inicial igual a 1 (um) tendo em vista tratarem dos serviços de implantação das soluções, os demais itens serão contratados após a implantação das soluções, conforme consta no item 7 DO CRONOGRAMA DE EVENTOS;

5.3. Quanto às unidades registradas:

5.3.1. Os itens 1 a 62, 67 e 68 referem-se a contratação de serviços para o período de 24 meses, conforme a seguir:

5.3.1.1. Itens 1 a 26: provimento de 1 (um) link MPLS por item por 24 meses cada link;

5.3.1.2. Item 27: provimento de 2 (dois) links MPLS por 24 meses cada link;

5.3.1.3. Item 28: aluguel de 2 (dois) roteadores por 24 meses cada roteador;

5.3.1.4. Itens 29 a 54: provimento de 1 (um) link de internet por item por 24 meses cada link;

5.3.1.5. Item 55: aluguel de 16 (dezesseis) soluções (Appliance de Firewall/Filtro de Conteúdo) por 24 meses cada solução, referentes às mesmas regionais com links tipo 1;

5.3.1.6. Item 56: aluguel de 7 (sete) soluções (Appliance de Firewall/Filtro de Conteúdo) por 24 meses cada solução, referentes às mesmas regionais com links tipo 2;

5.3.1.7. Item 57: aluguel de 3 (três) soluções (Appliance de Firewall/Filtro de Conteúdo) por 24 meses cada solução, referentes às mesmas regionais com links tipo 3;

5.3.1.8. Item 58: aluguel de 2 (duas) soluções (Appliance de Firewall/Filtro de Conteúdo) por 24 meses cada solução;

5.3.1.9. Itens 59 e 60: provimento de 1 (um) sistemas por item por 24 meses cada sistema;

5.3.1.10. Item 61: provimento de 1 (um) link internet por 24 meses;

5.3.1.11. Item 62: aluguel de 1 (um) roteador por 24 meses;

5.3.1.12. Item 67: provimento de 1 (um) link internet por 24 meses;

5.3.1.13. Item 68: aluguel de 1 (um) roteador por 24 meses.

5.3.2. O item 63 possui registrado o quantitativo de 12 (doze) serviços de mudança de endereço, referindo-se à expectativa de uso máximo do serviço de mudança dentro do período de vigência do contrato;

5.3.2.1. A renovação da vigência do contrato referente ao item 63 não implica em renovação do quantitativo contratado, mas apenas do período para uso dos quantitativos contratados;

5.3.2.2. Entende-se por serviço de mudança a mudança de endereços de instalação dos equipamentos e acessos dentro da mesma cidade;

5.3.2.3. Os serviços serão solicitados por meio de Ordem de Serviço.

5.3.3. Os itens 65, 66 e 70 possuem, cada, quantitativo registrado igual 1 (um) referindo-se a turmas de transferência de conhecimento a ser contratadas conforme conveniência da CONTRATANTE;

5.4. Quanto às faixas de serviço:

5.4.1. Os itens 1 a 27, 29 a 54, 61 e 67 possuem 5 (cinco) faixas pré-definidas, conforme detalhado no anexo I e visualizado na tabela 7. A CONTRATANTE se reserva ao direito de alterar individualmente as velocidades dos links dentro dessas faixas conforme sua necessidade durante toda a vigência do contrato;

5.4.1.1. Os serviços serão inicialmente prestados e pagos à CONTRATADA observando a faixa 1 de cada serviço;

5.4.1.2. A CONTRATANTE poderá a qualquer momento solicitar, via ordem de serviço, a alteração do serviço indicando nova faixa a ser fornecida, inclusive para uma faixa inferior;

5.4.1.3. Para fins de definição do valor do contrato e para a definição da licitante vencedora do certame será considerado o valor da faixa intermediária (faixa 4).

6. DAS ESPECIFICAÇÕES TÉCNICAS

6.1. As especificações técnicas referentes aos itens serviços contratados encontram-se no Anexo I deste Termo de Referência;

7. DO CRONOGRAMA DE EVENTOS

7.1. Itens 1 a 62 do lote 1 e itens 67 e 68 do lote 2: o cronograma abaixo disciplina o início do fornecimento dos serviços de comunicação que abrangem a infraestrutura da Rede WAN MPLS da CGU incluindo o link principal de Internet e os links regionais (lote 1: itens 1 a 62), e o início do fornecimento do link secundário de Internet (lote 2: itens 67 e 68);

7.1.1. Deverão ser apropriados neste contrato os custos referentes aos equipamentos utilizados no provimento do serviço;

7.1.2. O início do provimento dos serviços obedecerá ao cronograma abaixo:

Evento	Descrição do evento	Prazo Máximo	Responsável
1	Assinatura do contrato	-	CGU
2	Início da prestação dos serviços	Evento 1 + 10 dias	CONTRATADA

Tabela 2 - Cronograma de instalação na ferramenta

7.1.3. Os períodos constantes da tabela acima são definidos em dias corridos.

7.2. Item 63 do lote1: refere-se ao serviço de mudança de endereço, fornecimento de instalação dos equipamentos e acessos dentro da mesma cidade;

7.2.1. O início do provimento dos serviços obedecerá ao cronograma abaixo:

Evento	Descrição do evento	Prazo Máximo	Responsável
1	Envio de ordem de serviço para mudança de endereço	-	CGU
2	Finalização de mudança de endereço	Evento 1 + 60 dias	CONTRATADA

Tabela 1 - Cronograma de instalação na ferramenta

7.2.2. Os períodos constantes da tabela acima são definidos em dias corridos.

7.3. Item 64 do lote 1 e item 69 do lote 2: o cronograma abaixo disciplina a implantação de toda infraestrutura da Rede WAN MPLS da CGU (lote 1, item 64) e a implantação do link secundário de Internet da CGU (lote 2, item 69);

Evento	Descrição do evento	Prazo Máximo	Responsável
1	Assinatura do contrato e Assinatura do Termo de Confidencialidade	-	CONTRATADA e CONTRATANTE
2	Entrega do Plano de Implantação	Evento 1 + 10 dias	CONTRATADA
3	Avaliação do Plano de Implantação	Evento 2 + 5 dias	CONTRATANTE
4	Ajustes no Plano de Implantação	Evento 3 + 5 dias	CONTRATADA
5	Execução do Plano de Implantação da Solução de Gerenciamento de Serviços de TI	Evento 4 + 90 dias	CONTRATADA
6	Entrega da Documentação de Configuração “as built”	Evento 5 + 10 dias	CONTRATADA
7	Testes de Conformidade	Evento 6 + 30 dias	CONTRATADA e CONTRATANTE
8	Ajustes da não Conformidade	Evento 7 + 5 dias	CONTRATADA
9	Emissão do Termo de Recebimento Definitivo e início da execução dos serviços de suporte técnico	Após término do Evento 8 + 10 dias	CONTRATADA e CONTRATANTE

Tabela 4 - Cronograma de instalação na ferramenta

7.3.1. Os períodos constantes da tabela acima são definidos em dias corridos.

7.4. Itens 65 e 66 do lote 1 e item 70: cronograma disciplina o fornecimento de transferência de conhecimento no uso das tecnologias referenciados pelos itens 65, 66 (lote 1) e 70 (lote 2);

7.4.1. O provimento dos serviços obedecerá ao cronograma abaixo;

Evento	Descrição do evento	Prazo Máximo	Responsável
1	Assinatura do contrato	-	CONTRATADA e CONTRATANTE
2	Demanda serviço à contratada	-	CONTRATANTE
3	Apresenta cronograma	Evento 2 + 5 dias	CONTRATADA
4	Aprova cronograma	Evento 3 + 5 dias	CONTRATANTE
5	Realiza serviço de transferência de conhecimento	Conforme cronograma apresentado	CONTRATADA
6	Avalia serviço prestado	Evento 5 + 10 dias	CONTRATANTE
7	Emissão do Termo de Recebimento Definitivo referente ao serviço prestado	Evento 6 + 10 dias	CONTRATANTE

Tabela 5 - Cronograma de instalação na ferramenta

7.4.2. Os períodos constantes da tabela acima são definidos em dias corridos.

8. DOS NÍVEIS DE SERVIÇO

8.1. Os níveis de serviço referentes aos itens 1 a 63, 67 e 68 encontram-se no Anexo I deste Termo de Referência;

9. DO SUPORTE TÉCNICO

9.1. Este item define os requisitos do suporte técnico para os itens 1 a 62, 67 e 68;

9.2. A CONTRATADA responderá por todas as não conformidades quanto à prestação dos serviços durante o período de vigência do contrato;

9.3. O suporte técnico deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

9.4. O suporte técnico deverá ser prestado nos endereços do Ministério da Transparência e Controladoria-Geral da União – CGU em todo o Brasil, ou no ambiente de rede da CONTRATADA, ou ainda em qualquer local específico que der causa a falhas na prestação do serviço;

9.5. O serviço de gerenciamento e suporte técnico deve atuar de forma pró-ativa, antecipando-se aos problemas na rede e garantindo a qualidade do serviço estabelecida conforme níveis de serviço, realizando abertura, acompanhamento e fechamento de chamados técnicos relacionados com indisponibilidade e desempenho nos serviços, operando em regime 24 horas por dia, 7 dias por semana, durante toda a vigência do contrato;

9.5.1. A CONTRATADA deverá disponibilizar à CGU telefone 0800 (ou DDD 61), ou e-mail ou um portal de gerenciamento; para abertura e acompanhamento de chamados.

9.6. Para operacionalização do disposto anteriormente, a CONTRATADA deverá informar os números de telefone, ou e-mails, ou área em sítio da Web disponíveis para a abertura dos chamados técnicos;

9.7. A CONTRADATA deverá enviar até o 5º (quinto) dia útil de cada mês, um e-mail para a CGU contendo planilha que inclua histórico dos chamados do mês anterior, e pelo menos as seguintes informações para cada chamado:

9.7.1. Número do chamado;

9.7.2. Data e forma de abertura e fechamento (incluindo o nome para os casos em que a abertura ou fechamento sejam feitas de forma manual);

9.7.3. Tempo CONTRATANTE e tempo CONTRATADA;

9.7.4. Principais tratativas e informações do chamado, incluindo data e hora em que foram registradas no chamado.

9.8. Caso a CONTRATADA disponibilize no portal de gerenciamento o histórico dos chamados com os dados acima citados, fica dispensado o envio do e-mail; O histórico de chamados deve ser disponibilizado por pelo menos 6 (seis) meses;

9.9. A CONTRATADA deve informar e manter atualizados os dados de contato (nome, telefone fixo, celular e e-mail) de todos os envolvidos na cadeia de recorrência/escalation para o uso da CGU em caso de não atendimento dos níveis de serviço; A informação e atualização pode ser feita por e-mail ou disponibilizada no portal de gerenciamento.

9.10. O suporte técnico ocorrerá sem qualquer ônus para a CGU, mesmo quando for necessária a atualização de equipamentos da CONTRATADA, o translado e a estada de técnicos da CONTRATADA ou qualquer outro tipo de serviço necessário para garantir o cumprimento do serviço;

9.11. A CONTRATADA deverá disponibilizar à CGU um portal de gerenciamento; para acompanhamento dos níveis de serviço;

9.12. Entende-se por portal de gerenciamento, ferramenta acessível por intermédio de um navegador Web, com acesso restrito através de usuário/senha eletrônica e utilizando-se de protocolo HTTPS;

9.13. O portal de gerenciamento poderá ser constituído de um ou mais softwares e deverá prover, no mínimo, informações do último 1 (um) ano, com os valores instantâneos, médios e de pico, separados por mês, semana e dia, as seguintes informações:

9.13.1. Disponibilidade dos circuitos, em percentual;

9.13.2. Consumo de banda dos Links (entrada e saída);

9.13.3. Latências dos Links (ida e volta);

9.13.4. Perda de pacotes;

9.13.5. Quantidade de erros nas interfaces.

9.14. A indisponibilidade dos dados de gerenciamento (coleta não realizada, dados não acessíveis) será contabilizada como indisponibilidade do(s) serviço(s) associado(s), passível de desconto, no período em que os dados não forem coletados ou ficarem inacessíveis, caso isto implique em perda de dados de gerenciamento;

9.15. A CONTRATADA deverá manter todos os dados coletados dos elementos gerenciados e as informações geradas para confecção dos relatórios durante a vigência do contrato;

9.16. Os dados e informações armazenados, conjuntamente com o modelo de dados, poderão ser solicitados pela CGU, a qualquer tempo, à CONTRATADA que deverá disponibilizá-los no prazo máximo de 5 (cinco) dias úteis, em meio a ser definido pela CGU e/ou na base de dados da solução de gerência (carga dos dados extraídos e removidos);

9.17. O atendimento obedecerá aos prazos abaixo descritos:

9.17.1. Severidade MUITO ALTA: Esse nível de severidade é aplicado quando existe indisponibilidade no uso dos serviços causados por incidentes relacionados à segurança da informação, como por exemplo: Ataques de negação de serviço;

Prazo de Solução Definitiva
1. (uma) hora

9.17.2. Severidade ALTA: Esse nível de severidade é aplicado quando há a indisponibilidade total no uso dos serviços;

9.17.2.1. Entende-se indisponibilidade total, a prestação de serviços inaproveitáveis, conformes os seguintes parâmetros:

9.17.2.1.1. Perda de pacotes de circuito MPLS e Internet ultrapassar 5 % (cinco por cento);

9.17.2.1.2. Latência de circuito MPLS (ida e volta) ultrapassar 300 ms (trezentos milissegundos);

9.17.2.1.3. Latência de circuito Internet (ida e volta) ultrapassar 100 ms (cem milissegundos).

Prazo de Solução Definitiva
2 (duas) horas

9.17.3. Severidade MÉDIA: Esse nível de severidade é aplicado quando há falha, simultânea ou não, no uso dos serviços, estando ainda disponíveis, porém apresentando problemas;

9.17.3.1. Entende-se por falha ou problemas, a prestação de serviço fora dos Níveis de Serviço, conformes os seguintes parâmetros:

9.17.3.1.1. Perda de circuito MPLS e Internet entre 1% (um porcento) e 5% (dez porcento);

9.17.3.1.2. Latência de circuito MPLS (ida e volta) entre 150 ms (cento e cinquenta milissegundos) e 300 ms (trezentos milissegundos);

9.17.3.1.3. Latência de circuito Internet (ida e volta) entre 65 ms (sessenta e cinco milissegundos) e 100 ms (cem milissegundos).

9.17.3.2. Indisponibilidade da Solução de Gerência dos e Appliances de Firewall/Filtro de Conteúdo.

Prazo de Solução Definitiva
4 (quatro) horas

9.17.4. Severidade BAIXA: Esse nível de severidade é aplicado para:

9.17.4.1. Situações que não afetem o desempenho e disponibilidade dos serviços;

9.17.4.2. Indisponibilidade de 1 (um) dos nós do cluster Appliance de Firewall/Filtro de Conteúdo - Sede;

9.17.4.3. Indisponibilidade da solução de Netflow;

9.17.4.4. Indisponibilidade do serviço de multicast.

Prazo de Solução Definitiva
24 (vinte e quatro) horas

9.17.5. Severidade MUITO BAIXA: Esse nível de severidade é aplicado para:

9.17.5.1. Alteração nas configurações globais dos equipamentos (ALCs, prefix-list; NTP, SSH, SNMP, Syslog, DHCP Relay, prefix delegation, VLANs, distribute-lists, hostname, VRRP, BGP, OSPF, entre outros);

9.17.5.2. Solicitações de alteração nas configurações em regras de QoS que não envolvam ajuste nos PEs;

9.17.5.3. Inclusão/exclusão de usuários no Sistema de Gerência.

Prazo de Solução Definitiva
5 (cinco) dias úteis

9.17.6. Prestação de Esclarecimentos Técnicos e outras situações especiais: Esse nível de severidade é aplicado para:

9.17.6.1. Quando a CGU solicitar formalmente esclarecimentos técnicos relativos às ocorrências, ao uso e ao aprimoramento dos serviços;

9.17.6.2. Alteração nas configurações em regras de QoS que envolvam ajuste nos PEs;

9.17.6.3. Atualizações de software e firmware dos equipamentos.

Prazo de Resposta
15 (quinze) dias úteis

9.18. A contagem do prazo de solução definitiva de cada chamado iniciar-se-á a partir da abertura do chamado, em um dos canais de atendimento disponibilizados pela CONTRATADA, até o momento da comunicação da resolução definitiva do problema e o aceite pela equipe técnica da CGU;

9.19. A duração do chamado que será considerada para descontos será a soma dos períodos em que o chamado estiver sob responsabilidade da CONTRATADA. Ou seja, não serão computados os intervalos em que o chamado estiver sob responsabilidade da CGU, seja para avaliação dos resultados, seja para situações de observação ou qualquer outra situação em que a CGU solicite que o chamado fique no estado de aguardando ou "on hold";

9.20. Após concluído o chamado, a CONTRATADA comunicará o fato à equipe técnica da CGU e solicitará autorização para o fechamento do mesmo. Caso a CGU não confirme que o problema foi de fato resolvido, o chamado permanecerá aberto até que seja efetivamente solucionado. Neste caso, a CGU fornecerá as pendências relativas ao chamado aberto. Em hipótese alguma a CONTRADA poderá proceder com o fechamento do chamado sem a anuência explícita da CGU;

10. DAS SANÇÕES

10.1. A não observância pela CONTRATADA quanto aos prazos estabelecidos neste termo referentes aos quesitos de suporte definidos no item 9. DO SUPORTE TÉCNICO resulta na sujeição da CONTRATADA às sanções abaixo definidas:

Resultado esperados e níveis de qualidade exigidos	Unidade de cálculo	Fórmula de cálculo da multa	Limite da multa por infração
1 – Muito Alta	1 hora	**NHAT** * 4,0% * **VMI**	10% da **VMF**
2 – Alta	1 hora	**NHAT** * 2,0% * **VMI**	10% da **VMF**
3 – Média	1 hora	**NHAT** * 1,0% * **VMI**	10% da **VMF**
4 – Baixo	1 hora	**NHAT** * 0,5% * **VMI**	10% da **VMF**
5 – Muito Baixa	1 dia	**NDAT** * 5,0% * **VMI**	10% da **VMF**
6 – Esclarecimentos e outras situações especiais	1 dia	**NDAT** * 5,0% * **VMI**	10% da **VMF**

Tabela 6 – Sanções referentes a quesitos de suporte técnico

Em que:

VMI: Valor mensal do item;

VMF: Valor mensal da fatura;

NHAT: número de horas decorridas após o término de atendimento.

NDAT: número de dias decorridos após o término de atendimento.

10.1.1. Para finalidade de aplicação de sanção, o VMI referente aos itens 55 a 59 considerará a proporcionalidade referente de cada regional afetada no valor do item contratado;

10.1.1.1. Por exemplo, o VMI referente um appliance com mal funcionamento referente ao item 55, será 1/16 (um dezesseis avos) do valor contratado para o referido item.

10.2. A não observância pela CONTRATADA quanto aos prazos estabelecidos neste termo para implantação da solução, itens 64 e 69, resulta na sujeição da CONTRATADA às sanções abaixo definidas:

10.2.1. Advertência: Atraso injustificado em até sete dias corridos;

10.2.2. Multa: Atraso injustificado em período maior de sete dias corridos. O valor da multa a ser aplicado será calculado conforme abaixo:

$$VM = [(NDA – 7) * VC* 0,1] / 60$$

VM = Valor da multa;

NDA = Número de dias (corridos) atrasados;

VC = Valor contratado para o quantitativo de itens atrasados;

O valor máximo da multa será equivalente a 60 dias de atrasos. A partir deste momento, e de forma acumulativa, se aplica a penalidade de impedimento de licitar e contratar com a União, Estados, Distrito Federal ou Municípios, conforme próximos subitem;

10.3. A não observância pela CONTRATADA quanto aos prazos estabelecidos neste termo para serviço de transferência de conhecimento, itens 65, 66 e 70, resulta na sujeição da CONTRATADA às sanções abaixo definidas:

10.3.1. Advertência: Atraso injustificado em até sete dias corridos;

10.3.2. Multa: Atraso injustificado em período maior de sete dias corridos. O valor da multa a ser aplicado será calculado conforme abaixo:

$$VM = [(NDA – 7) * VC* 0,1] / 21$$

VM = Valor da multa;

NDA = Número de dias (corridos) atrasados;

VC = Valor contratado para o quantitativo de itens atrasados;

O valor máximo da multa será equivalente a 21 dias de atrasos;

10.4. A não observância pela CONTRATADA quanto aos prazos estabelecidos neste termo para serviço de mudança de endereço, item 63, resulta na sujeição da CONTRATADA às sanções abaixo definidas:

10.4.1. Advertência: Atraso injustificado em até sete dias corridos;

10.4.2. Multa: Atraso injustificado em período maior de sete dias corridos. O valor da multa a ser aplicado será calculado conforme abaixo:

$$VM = [(NDA – 7) * VC* 0,1] / 30$$

VM = Valor da multa;

NDA = Número de dias (corridos) atrasados;

VC = Valor contratado para o quatitativo de itens atrasados;

O valor máximo da multa será equivalente a 30 dias de atrasos.

11. DAS OBRIGAÇÕES DA CONTRATADA

11.1. Tomar todas as providências necessárias à fiel execução do objeto do Contrato;

11.2. Atender prontamente quaisquer orientações e exigências do Gestor do Contrato, inerentes à execução do objeto contratual que sejam em conformidade com as previsões editalícias, contratuais ou legais;

11.3. Promover a execução do objeto dentro dos parâmetros contratuais estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica;

11.4. Refazer todos os serviços que forem considerados insatisfatórios perante os parâmetros contratuais estabelecidos, sem que caiba qualquer acréscimo no custo contratado;

11.5. Prestar todos os esclarecimentos que lhe forem solicitados pela CONTRATANTE, atendendo prontamente a quaisquer reclamações;

11.6. Propiciar todos os meios e facilidades necessárias à fiscalização dos serviços pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;

11.7. Manter, durante o período de vigência do contrato, todas as condições de habilitação e qualificação exigidas na licitação;

11.8. Responder integralmente pelos danos causados, direta ou indiretamente, ao patrimônio da União, ou a terceiros, em decorrência de ação ou omissão de seus representantes legais, empregados ou prepostos, não se excluindo ou reduzindo essa responsabilidade em razão da fiscalização ou do acompanhamento realizado pela CONTRATANTE;

11.9. Arcar com os ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de contravenção, seja por culpa sua ou de quaisquer de seus empregados ou prepostos, obrigando-se, outrossim, a quaisquer responsabilidades decorrentes de ações judiciais ou extrajudiciais de terceiros, que lhe venham a ser exigidas por força da lei, ligadas ao cumprimento do contrato;

11.10. Assumir todos os encargos de possível demanda trabalhista, cível ou penal, relacionados à execução do objeto, originariamente ou vinculada por prevenção, conexão ou contingência;

11.11. Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, uma vez que os seus empregados não manterão nenhum vínculo empregatício com a CONTRATANTE;

11.12. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados quando execução do objeto ou em conexão com ele, ainda que acontecido em dependência da CONTRATANTE, inclusive por danos causados a terceiros;

11.13. Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes da adjudicação do processo licitatório;

11.14. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto, devendo orientar seus empregados nesse sentido;

11.15. Providenciar que seus contratados portem crachá de identificação quando da execução do objeto à CONTRATANTE;

11.16. Aceitar, nas mesmas condições do ajuste, os acréscimos ou supressões que se fizerem no objeto, de até 25% (vinte e cinco por cento) do valor do contrato.

12. DAS OBRIGAÇÕES DA CONTRATANTE

12.1. Nomear Gestor do Contrato, assim como Fiscais Técnico, Administrativo e Requisitante para acompanhar e fiscalizar a execução dos contratos;

12.2. Permitir o livre acesso dos empregados da CONTRATADA às dependências da CONTRATANTE, para prestação de serviço;

12.3. Atestar as faturas correspondentes, por intermédio de servidor competente;

12.4. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em Contrato;

12.5. Efetuar o pagamento devido pelos serviços prestados, no prazo estabelecido, desde que cumpridas todas as formalidades e exigências previstas;

12.6. Comunicar oficialmente, por escrito, à CONTRATADA quaisquer falhas verificadas no curso do fornecimento dos equipamentos e eventual prestação de assistência técnica ou suporte, determinando o que for necessário à sua regularização.

12.7. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis;

12.8. Encaminhar formalmente a demanda, preferencialmente por meio de Ordem de Serviço, de acordo com os critérios estabelecidos neste Termo de Referência;

12.9. Realizar, no momento da licitação, diligências com o licitante classificado provisoriamente em primeiro lugar, para fins de comprovação de atendimento das especificações.

13. DA SUBCONTRATAÇÃO

13.1. Será permitida a subcontratação para o fornecimento de Link da última milha dos Links das unidades regionais;

13.2. Será permitida a subcontratação dos itens de repasse de conhecimento.

14. DA HABILITAÇÃO

14.1. Além das exigências administrativas e legais especificadas no Edital, a empresa deverá apresentar juntamente com a documentação de habilitação os seguintes atestados/declarações:

14.2. Quanto ao Lote 01:

14.2.1. Declaração ou Atestado de Capacidade Técnico-Operacional, fornecido por pessoa jurídica de direito público ou privado, que comprove que o licitante prestou ou tem prestado, satisfatoriamente, pelo período mínimo de 12 (doze) meses, o serviço de rede WAN MPLS (Multiprotocol Label Switching), em nível nacional, com interligação de, no mínimo, 13 (treze) unidades da federação com Links iguais ou superiores a 2 Mbps;

14.2.1.1. Não será aceito o somatório de declarações e/ou atestados para fins de comprovação de cada deste critério técnico tendo em vista a necessidade de aferir a capacidade de provimento de serviço de telecomunicação com abrangência nacional por meio de backbone próprio;

14.2.1.1.1. Os quantitativos exigidos representam aproximadamente 50% da demanda da CGU com relação ao número de unidades da federação e 50% da demanda da CGU com relação à taxa de transmissão mínima estabelecida no Anexo I deste Termo de Referência.

14.2.2. Declaração ou Atestado de Capacidade Técnico-Operacional, fornecido por pessoa jurídica de direito público ou privado, que comprove que o licitante prestou ou tem prestado, satisfatoriamente, pelo período mínimo de 12 (doze) meses, o serviço de Link de Internet com Link igual ou superior a 50 Mbps, incluindo o serviço de anti-DDoS.

14.2.2.1. Considerou-se a taxa mínima de 50 Mbps, 1/3 da menor taxa a ser fornecida, como critério suficiente para aferimento da capacidade do proponente.

14.3. Quanto ao Lote 02:

14.3.1. Declaração ou Atestado de Capacidade Técnico-Operacional, fornecido por pessoa jurídica de direito público ou privado, que comprove que o licitante prestou ou tem prestado, satisfatoriamente, pelo período mínimo de 12 (doze) meses, o serviço de Link de Internet com Link igual ou superior a 50 Mbps, incluindo o serviço de anti-DDoS.

14.3.1.1. Considerou-se a taxa mínima de 50 Mbps, 1/3 da menor taxa a ser fornecida, como critério suficiente para aferimento da capacidade do proponente.

14.4. Será aceito o somatório de declarações e/ou atestados para fins de comprovação de prestação de serviço pelo período mínimo de 12 (doze) meses, sendo exigido que esses atestados/declarações sejam referentes a contratos executados em períodos distintos (períodos concomitantes serão computados uma única vez);

14.5. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução;

14.6. Os atestados de capacidade técnico-operacional deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente, exceto se firmado para ser executado em prazo inferior;

14.7. A CONTRATANTE poderá realizar diligência/visita técnica, a fim de se comprovar a veracidade do(s) Atestado(s) de Capacidade Técnica apresentado(s) pela LICITANTE, quando, poderá ser requerida cópia do(s) contrato(s), nota(s) fiscal(is) ou qualquer outro documento que comprove inequivocamente que o serviço apresentado no(s) atestado(s) foi(ram) prestado(s).

15. DA GARANTIA CONTRATUAL

15.1. Serão exigidas garantias contratuais no valor de 3% do valor total dos respectivos contratos;

15.1.1. Não serão exigidas garantias contratuais para os serviços referentes ao itens 65, 66 e 70.

16. DA PROPRIEDADE, SIGILO E SEGURANÇA DAS INFORMAÇÕES

16.1. Os executores da CONTRATADA que atuarão na implantação e nos demais serviços previstos, receberão acesso privativo e individualizado, não podendo repassá-los a terceiros, sob pena de responder, criminalmente e judicialmente, pelos atos e fatos que venham a ocorrer, em decorrência deste ilícito;

16.2. Será considerado ilícito a divulgação, o repasse ou utilização indevida de informações, bem como dos documentos, imagens, gravações e informações utilizados durante a prestação dos serviços;

16.3. A CONTRATADA obriga-se a dar ciência à CONTRATANTE, imediatamente e por escrito, sobre qualquer anormalidade que verificar na prestação dos serviços;

16.4. A CONTRATADA deverá guardar inteiro sigilo dos dados processados, reconhecendo serem estes de propriedade exclusiva da CONTRATANTE, sendo vedada à CONTRATADA sua cessão, locação ou venda a terceiros sem prévia autorização formal da CONTRATANTE, de acordo com os termos constantes do Anexo XI – Modelo de Termo de Confidencialidade;

16.5. Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer reprodução, utilização ou divulgação a terceiros, devendo a CONTRATADA zelar por si e por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados;

16.6. Cada profissional a serviço da CONTRATADA deverá estar ciente de que a estrutura computacional da CONTRATANTE não poderá ser utilizada para fins particulares. O correio eletrônico fornecido pela CONTRATANTE, bem como a navegação em sítios da Internet ou acessadas a partir dos seus equipamentos poderão ser auditados;

16.7. A CONTRATADA deverá entregar à CONTRATANTE toda e qualquer documentação produzida decorrente da prestação de serviços, objeto desta licitação, bem como, cederá à CONTRATANTE, em caráter definitivo e irrevogável, o direito patrimonial e a propriedade intelectual dos resultados produzidos durante a vigência do contrato e eventuais aditivos, entendendo-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e documentação, em papel ou em qualquer forma ou mídia.

17. DA VIGÊNCIA DO CONTRATO

17.1. Os contratos referentes aos serviços de instalação, itens 64 (lote 1) e 69 (lote 2), terão vigência de 330 dias corridos a partir da data de sua assinatura;

17.1.1. Os contratos poderão ser prorrogados por igual período, nos termos do art. 57, §1º, da Lei nº 8.666/93.

17.2. Os contratos referentes ao provimento dos serviços de infraestrutura de rede, itens 1 a 63 (lote 1) e 67 a 68 (lote 2), terão vigência de 24 (vinte e quatro) meses, contados a partir da sua assinatura;

17.2.1. Os contratos poderão ser prorrogados por mais um período de 24 (vinte e quatro) meses e outro 12 (doze) meses, até o limite de vigência total de 60 (sessenta) meses, desde que mantida a obtenção de preços e condições mais vantajosas para a Administração, nos termos do Artigo 57, Inciso II, da Lei nº 8.666/1993;

17.2.2. Os itens 65 e 66 (lote 1) e 70 (lote 2) poderão constar também destes contratos ou em contratos próprios, conforme conveniência da CONTRATANTE;

17.2.2.1. Caso constem de contratos específicos, estes terão vigência de 120 dias corridos a partir da data de sua assinatura.

18. DO PAGAMENTO DA DESPESA

18.1. Os pagamentos dos itens 64, 65, 66, 69 e 70 da Tabela 1 dar-se-ão em parcela única e dependerão do recebimento definitivo pela equipe técnica da CGU, formalizado por meio do respectivo Termo de Aceite, e que será lavrado após verificação da adequação dos produtos serviços perante às especificações exigidas;

18.2. Os pagamentos referentes ao item 63 da Tabela 1 dar-se-ão em uma única parcela para cada mudança de endereço realizada e dependerão do recebimento definitivo pela equipe técnica da CGU, formalizado por meio do respectivo Termo de Aceite, e que será lavrado após verificação da adequação dos serviços às especificações exigidas;

18.3. O pagamento dos serviços, itens 1 a 62, 67 e 68 da Tabela 1, dar-se-á mensalmente, após a formalização do aceite da Nota Fiscal/Fatura pela equipe técnica da CGU, devendo o valor ser pago ao final de cada período de prestação do serviço já com os descontos aplicados em função do não cumprimento dos níveis mínimos de serviço e de demais sanções cabíveis;

18.3.1. Os valores serão pagos conforme faixa de serviço definida previamente pela CONTRATANTE:

18.3.2. Os serviços serão inicialmente prestados e pagos à CONTRATADA observando a faixa 1 de cada serviço, conforme tabela 7;

18.3.3. Os níveis mínimos de serviço a serem observados são definidos no Anexo II.

18.4. O pagamento será efetuado à CONTRATADA, por intermédio de Ordem Bancária, emitida no prazo de até 10 (dez) dias úteis, contados do recebimento da Nota Fiscal/Fatura, compreendida nesse período a fase de ateste da mesma - a qual conterá o endereço, o CNPJ, o número da Nota de Empenho, os números do Banco, da Agência e da Conta Corrente da empresa, a descrição clara do objeto do contrato - em moeda corrente nacional, por intermédio de Ordem Bancária e de acordo com as condições constantes na proposta da empresa e aceitas pela CONTRATANTE;

18.5. Para execução do pagamento de que trata este subitem, a CONTRATADA deverá fazer constar como beneficiário/cliente da Nota Fiscal/Fatura correspondente, emitida sem rasuras, ao Ministério da Transparência e Controladoria-Geral da União, CNPJ nº 26.664.015/0001-48;

18.6. Caso a CONTRATADA seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, desde que não haja vedação legal para tal opção em razão do objeto executado, a mesma deverá apresentar, juntamente com a Nota Fiscal/Fatura, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor;

18.7. A emissão da Ordem Bancária será efetuada dentro do prazo estipulado no subitem 18.4, somente após a Nota Fiscal/Fatura ser conferida, aceita e atestada por servidor responsável e ter sido verificada a regularidade da CONTRATADA, mediante consulta on-line ao Sistema Unificado de Cadastro de Fornecedores – SICAF e às demais Certidões (CEIS, CNJ E CNDT) para comprovação, dentre outras coisas, do devido recolhimento das contribuições sociais (FGTS e Previdência Social) e demais tributos estaduais e federais, conforme cada caso;

18.8. Os respectivos documentos de consulta ao SICAF e às demais Certidões do subitem anterior deverão ser anexados ao processo de pagamento;

18.9. Havendo erro na Nota Fiscal/Fatura ou circunstância que impeça a liquidação da despesa, aquela será devolvida pelo Fiscal à CONTRATADA e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento se reiniciará após a regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para a CONTRATANTE;

18.10. Constatada a situação de irregularidade da CONTRATADA no SICAF, ela será notificada, por escrito, sem prejuízo do pagamento pelo objeto já executado, para, num prazo de 05 (cinco) dias úteis, regularizar tal situação ou, no mesmo prazo, apresentar defesa, sob pena de rescisão do Contrato;

18.10.1. O prazo para regularização ou encaminhamento de defesa de que trata o subitem anterior poderá ser prorrogado uma vez e por igual período, a critério da CONTRATANTE;

18.10.2. Não havendo regularização ou sendo a defesa considerada improcedente, a Administração deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal e trabalhista quanto à inadimplência do fornecedor, bem como quanto à existência de pagamento a ser efetuado pela Administração, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos;

18.10.3. Persistindo a irregularidade, a Administração deverá adotar as medidas necessárias à rescisão contratual em execução, nos autos dos processos administrativos correspondentes, assegurada à CONTRATADA a ampla defesa;

18.10.4. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão contratual, caso a CONTRATADA não regularize sua situação junto ao SICAF;

18.10.5. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do órgão ou entidade contratante, não será rescindido o contrato em execução com empresa ou profissional inadimplente no SICAF.

18.11. A critério da CONTRATANTE poderão ser utilizados os créditos existentes em favor da CONTRATADA para compensar quaisquer possíveis despesas resultantes de multas, indenizações, inadimplências contratuais e/ou outras de responsabilidade desta última;

18.12. No caso de eventual atraso de pagamento, e mediante pedido da CONTRATADA, o valor devido será atualizado financeiramente, desde a data a que o mesmo se referia até a data do efetivo pagamento, pelo Índice de Preços ao Consumidor Amplo – IPCA, mediante aplicação da seguinte fórmula:

AF = [(1 + IPCA/100)N/30 –1] x VP, onde:

AF= atualização financeira;

IPCA= percentual atribuído ao Índice de Preços ao Consumidor Amplo, com vigência a partir da data do adimplemento da etapa;

N= número de dias entre a data do adimplemento da etapa e a do efetivo pagamento;

VP= valor da etapa a ser paga, igual ao principal mais o reajuste.

19. DOS PREÇOS DOS SERVIÇOS DE INFRAESTURURA DE REDE E INTERNET

19.1. Os contratos referentes à prestação de serviço abrangem provimento de serviços que poderão ser demandados dentro de faixas definidas na tabela 7, conforme Anexo I;

19.2. O Anexo I traz para os itens 1 a 27, 29 a 54, 61 e 67 a definição das menores e maiores taxas de transmissão que poderão ser fornecidas no âmbito do contrato;

19.3. O preço para o serviço prestado será calculado conforme a seguinte fórmula:

$$PS = VMbps * VNP * (1 – Df)^{(VNP – 1)}$$

PS = Preço do Serviço;

VMbps = Valor unitário do Mbps;

VNP = Velocidade nominal provida, em Mbps;

Df = Valor do deflator utilizado.

19.4. Os valores dos deflatores a serem utilizados são:

19.4.1. Deflator link MPLS regional: 1,90%;

19.4.2. Deflator link MPLS Sede: 0,05%;

19.4.3. Deflator link Internet regional: 1,90%;

19.4.4. Deflator link Internet Sede: 0,05%.

20. DA ESTIMATIVA DA DESPESA

Lote	Item	Descrição	Qtd Inicial	Qtd Registrada	Unidade	Valor Unitário	Faixa 1 (Mbps)	Valor mensal Faixa 1	Faixa 2 (Mbps)	Valor mensal Faixa 2	Faixa 3 (Mbps)	Valor mensal Faixa 3	Faixa 4 (Mbps)	Valor mensal Faixa 4	Faixa 5 (Mbps)	Valor mensal Faixa 5	Valor de Referência	Valor Total 24 Meses	
1	1	Link MPLS - Regional Tipo 1 - AC	0	**24**	Mês	216,72	4	818,40	6	1.181,40	8	1.515,91	10	1.823,56	12	2.105,91	1.823,56	43.765,44	
	2	Link MPLS - Regional Tipo 1 - AL	0	**24**	Mês	233,06	4	880,11	6	1.270,47	8	1.630,20	10	1.961,05	12	2.264,69	1.961,05	47.065,20	
	3	Link MPLS - Regional Tipo 1 - AM	0	**24**	Mês	233,06	4	880,11	6	1.270,47	8	1.630,20	10	1.961,05	12	2.264,69	1.961,05	47.065,20	
	4	Link MPLS - Regional Tipo 1 - AP	0	**24**	Mês	229,60	4	867,04	6	1.251,61	8	1.606,00	10	1.931,94	12	2.231,06	1.931,93	46.366,32	
	5	Link MPLS - Regional Tipo 1 - ES	0	**24**	Mês	216,72	4	818,40	6	1.181,40	8	1.515,91	10	1.823,56	12	2.105,91	1.823,56	43.765,44	
	6	Link MPLS - Regional Tipo 1 - MA	0	**24**	Mês	229,60	4	867,04	6	1.251,61	8	1.606,00	10	1.931,94	12	2.231,06	1.931,93	46.366,32	
	7	Link MPLS - Regional Tipo 1 - MS	0	**24**	Mês	229,60	4	867,04	6	1.251,61	8	1.606,00	10	1.931,94	12	2.231,06	1.931,93	46.366,32	
	8	Link MPLS - Regional Tipo 1 - MT	0	**24**	Mês	240,30	4	907,45	6	1.309,94	8	1.680,84	10	2.021,97	12	2.335,04	2.021,97	48.527,28	
	9	Link MPLS - Regional Tipo 1 - PB	0	**24**	Mês	233,06	4	880,11	6	1.270,47	8	1.630,20	10	1.961,05	12	2.264,69	1.961,05	47.065,20	
	10	Link MPLS - Regional Tipo 1 - PI	0	**24**	Mês	216,72	4	818,40	6	1.181,40	8	1.515,91	10	1.823,56	12	2.105,91	1.823,56	43.765,44	
	11	Link MPLS - Regional Tipo 1 - RN	0	**24**	Mês	233,06	4	880,11	6	1.270,47	8	1.630,20	10	1.961,05	12	2.264,69	1.961,05	47.065,20	
	12	Link MPLS - Regional Tipo 1 - RO	0	**24**	Mês	222,97	4	842,00	6	1.215,47	8	1.559,62	10	1.876,15	12	2.166,64	1.876,14	45.027,36	
	13	Link MPLS - Regional Tipo 1 - RR	0	**24**	Mês	216,72	4	818,40	6	1.181,40	8	1.515,91	10	1.823,56	12	2.105,91	1.823,56	43.765,44	
	14	Link MPLS - Regional Tipo 1 - SC	0	**24**	Mês	216,72	4	818,40	6	1.181,40	8	1.515,91	10	1.823,56	12	2.105,91	1.823,56	43.765,44	
	15	Link MPLS - Regional Tipo 1 - SE	0	**24**	Mês	233,06	4	880,11	6	1.270,47	8	1.630,20	10	1.961,05	12	2.264,69	1.961,05	47.065,20	
	16	Link MPLS - Regional Tipo 1 - TO	0	**24**	Mês	229,60	4	867,04	6	1.251,61	8	1.606,00	10	1.931,94	12	2.231,06	1.931,93	46.366,32	
	17	Link MPLS - Regional Tipo 2 - BA	0	**24**	Mês	267,70	6	1.459,30	8	1.872,50	10	2.252,52	12	2.601,29	14	2.920,61	2.601,28	62.430,72	
	18	Link MPLS - Regional Tipo 2 - CE	0	**24**	Mês	275,77	6	1.503,29	8	1.928,95	10	2.320,43	12	2.679,71	14	3.008,65	2.679,70	64.312,80	
	19	Link MPLS - Regional Tipo 2 - GO	0	**24**	Mês	271,68	6	1.481,00	8	1.900,34	10	2.286,01	12	2.639,96	14	2.964,03	2.639,96	63.359,04	

20	Link MPLS - Regional Tipo 2 - PA	0	**24**	Mês	275,77	6	1.503,29	8	1.928,95	10	2.320,43	12	2.679,71	14	3.008,65	2.679,70	64.312,80	
21	Link MPLS - Regional Tipo 2 - PE	0	**24**	Mês	275,77	6	1.503,29	8	1.928,95	10	2.320,43	12	2.679,71	14	3.008,65	2.679,70	64.312,80	
22	Link MPLS - Regional Tipo 2 - PR	0	**24**	Mês	271,68	6	1.481,00	8	1.900,34	10	2.286,01	12	2.639,96	14	2.964,03	2.639,96	63.359,04	
23	Link MPLS - Regional Tipo 2 - RS	0	**24**	Mês	275,77	6	1.503,29	8	1.928,95	10	2.320,43	12	2.679,71	14	3.008,65	2.679,70	64.312,80	
24	Link MPLS - Regional Tipo 3 - MG	0	**24**	Mês	288,18	8	2.015,75	10	2.424,85	12	2.800,30	14	3.144,05	16	3.457,95	3.144,04	75.456,96	
25	Link MPLS - Regional Tipo 3 - RJ	0	**24**	Mês	310,57	8	2.172,36	10	2.613,25	12	3.017,87	14	3.388,32	16	3.726,62	3.388,32	81.319,68	
26	Link MPLS - Regional Tipo 3 - SP	0	**24**	Mês	280,10	8	1.959,23	10	2.356,86	12	2.721,78	14	3.055,89	16	3.361,00	3.055,89	73.341,36	
27	2 (dois) Links MPLS - Sede – DF	0	24	Mês	529,85	50	25.851,23	100	50.425,61	150	73.770,44	200	95.931,45	250	116.952,89	95.931,45	2.302.354,80	
28	2 (dois) Roteadores MPLS – Sede	0	**24**	Mês	1.558,54	-	-	-	-	-	-	-	-	-	-	3.117,07	74.809,68	
29	Link Internet - Regional Tipo 1 - AC	0	**24**	Mês	177,76	6	969,03	10	1.495,76	14	1.939,40	18	2.309,34	22	2.614,05	2.309,34	55.424,16	
30	Link Internet - Regional Tipo 1 - AL	0	**24**	Mês	191,16	6	1.042,06	10	1.608,48	14	2.085,55	18	2.483,37	22	2.811,04	2.483,36	59.600,64	
31	Link Internet - Regional Tipo 1 - AM	0	**24**	Mês	191,16	6	1.042,06	10	1.608,48	14	2.085,55	18	2.483,37	22	2.811,04	2.483,36	59.600,64	
32	Link Internet - Regional Tipo 1 - AP	0	**24**	Mês	188,32	6	1.026,59	10	1.584,60	14	2.054,58	18	2.446,49	22	2.769,30	2.446,49	58.715,76	
33	Link Internet - Regional Tipo 1 - ES	0	**24**	Mês	177,76	6	969,03	10	1.495,76	14	1.939,40	18	2.309,34	22	2.614,05	2.309,34	55.424,16	
34	Link Internet - Regional Tipo 1 - MA	0	**24**	Mês	188,32	6	1.026,59	10	1.584,60	14	2.054,58	18	2.446,49	22	2.769,30	2.446,49	58.715,76	
35	Link Internet - Regional Tipo 1 - MS	0	**24**	Mês	188,32	6	1.026,59	10	1.584,60	14	2.054,58	18	2.446,49	22	2.769,30	2.446,49	58.715,76	
36	Link Internet - Regional Tipo 1 - MT	0	**24**	Mês	197,10	6	1.074,44	10	1.658,47	14	2.150,37	18	2.560,55	22	2.898,41	2.560,55	61.453,20	
37	Link Internet - Regional Tipo 1 - PB	0	**24**	Mês	191,16	6	1.042,06	10	1.608,48	14	2.085,55	18	2.483,37	22	2.811,04	2.483,36	59.600,64	
38	Link Internet - Regional Tipo 1 - PI	0	**24**	Mês	177,76	6	969,03	10	1.495,76	14	1.939,40	18	2.309,34	22	2.614,05	2.309,34	55.424,16	
39	Link Internet - Regional Tipo 1 - RN	0	**24**	Mês	191,16	6	1.042,06	10	1.608,48	14	2.085,55	18	2.483,37	22	2.811,04	2.483,36	59.600,64	
40	Link Internet - Regional Tipo 1 - RO	0	**24**	Mês	182,89	6	996,98	10	1.538,90	14	1.995,33	18	2.375,94	22	2.689,44	2.375,93	57.022,32	

41	Link Internet - Regional Tipo 1 - RR	0	**24**	Mês	177,76	6	969,03	10	1.495,76	14	1.939,40	18	2.309,34	22	2.614,05	2.309,34	55.424,16	
42	Link Internet - Regional Tipo 1 - SC	0	**24**	Mês	177,76	6	969,03	10	1.495,76	14	1.939,40	18	2.309,34	22	2.614,05	2.309,34	55.424,16	
43	Link Internet - Regional Tipo 1 - SE	0	**24**	Mês	191,16	6	1.042,06	10	1.608,48	14	2.085,55	18	2.483,37	22	2.811,04	2.483,36	59.600,64	
44	Link Internet - Regional Tipo 1 - TO	0	**24**	Mês	188,32	6	1.026,59	10	1.584,60	14	2.054,58	18	2.446,49	22	2.769,30	2.446,49	58.715,76	
45	Link Internet - Regional Tipo 2 - BA	0	**24**	Mês	170,73	8	1.194,22	12	1.659,02	16	2.048,64	20	2.371,66	24	2.635,78	2.371,66	56.919,84	
46	Link Internet - Regional Tipo 2 - CE	0	**24**	Mês	175,88	8	1.230,22	12	1.709,03	16	2.110,40	20	2.443,15	24	2.715,23	2.443,14	58.635,36	
47	Link Internet - Regional Tipo 2 - GO	0	**24**	Mês	173,27	8	1.211,95	12	1.683,65	16	2.079,06	20	2.406,87	24	2.674,92	2.406,87	57.764,88	
48	Link Internet - Regional Tipo 2 - PA	0	**24**	Mês	175,88	8	1.230,22	12	1.709,03	16	2.110,40	20	2.443,15	24	2.715,23	2.443,14	58.635,36	
‘’’	Link Internet - Regional Tipo 2 - PE	0	**24**	Mês	175,88	8	1.230,22	12	1.709,03	16	2.110,40	20	2.443,15	24	2.715,23	2.443,14	58.635,36	
50	Link Internet - Regional Tipo 2 - PR	0	**24**	Mês	173,27	8	1.211,95	12	1.683,65	16	2.079,06	20	2.406,87	24	2.674,92	2.406,87	57.764,88	
51	Link Internet - Regional Tipo 2 - RS	0	**24**	Mês	175,88	8	1.230,22	12	1.709,03	16	2.110,40	20	2.443,15	24	2.715,23	2.443,14	58.635,36	
52	Link Internet - Regional Tipo 3 - MG	0	**24**	Mês	158,42	10	1.333,03	14	1.728,40	18	2.058,10	22	2.329,66	26	2.549,87	2.329,65	55.911,60	
53	Link Internet - Regional Tipo 3 - RJ	0	**24**	Mês	170,73	10	1.436,61	14	1.862,70	18	2.218,01	22	2.510,67	26	2.748,00	2.510,66	60.255,84	
54	Link Internet - Regional Tipo 3 - SP	0	**24**	Mês	153,98	10	1.295,67	14	1.679,95	18	2.000,40	22	2.264,35	26	2.478,40	2.264,35	54.344,40	
55	16 (dezesseis) Appliances de Firewall/Filtro de Conteúdo - Regionais Tipo 1	0	**24**	Mês	13.920,00	-	-	-	-	-	-	-	-	-	-	13.920,00	334.080,00	
56	7 (sete) Appliances de Firewall/Filtro de Conteúdo - Regionais Tipo 2	0	**24**	Mês	8.799,00	-	-	-	-	-	-	-	-	-	-	8.799,00	211.176,00	
57	3 (três) Appliance de Firewall/Filtro de Conteúdo - Regionais Tipo 3	0	**24**	Mês	5.034,00	-	-	-	-	-	-	-	-	-	-	5.034,00	120.816,00	
58	2 (dois) Appliance de Firewall/Filtro de Conteúdo - Sede	0	**24**	Mês	13.200,00	-	-	-	-	-	-	-	-	-	-	13.200,00	316.800,00	

	59	Solução de Gerência dos e Appliances de Firewall/Filtro de Conteúdo	0	**24**	Mês	5.256,00	-	-	-	-	-	-	-	-	-	-	5.256,00	126.144,00	
	60	Solução de Netflow	0	**24**	Mês	6.530,00	-	-	-	-	-	-	-	-	-	-	6.530,00	156.720,00	
	61	Link Internet - Sede 1	0	**24**	Mês	175,11	150	24.380,31	200	31.704,28	250	38.651,63	300	45.236,49	350	51.472,55	45.236,49	1.085.675,76	
	62	Roteador Internet - Sede 1	0	**24**	Mês	1.081,60	-	-	-	-	-	-	-	-	-	-	1.081,60	25.958,40	
	63	Serviço de Mudança de Endereço	0	**12**	Serviço de mudança de Endereço	1.000,00	-	-	-	-	-	-	-	-	-	-	1.000,00	12.000,00	
	64	Implantação solução - Lote 1	1	**1**	Implantação	27.000,00	-	-	-	-	-	-	-	-	-	-	27.000,00	27.000,00	
	65	Repasse de Conhecimento - Solução Firewall/Filtro de Conteúdo	0	**1**	Turma	15.000,00	-	-	-	-	-	-	-	-	-	-	15.000,00	15.000,00	
	66	Repasse de Conhecimento - Roteador Internet - Sede 1	0	**1**	Turma	10.000,00	-	-	-	-	-	-	-	-	-	-	10.000,00	10.000,00	
2	67	Link Internet - Sede 2	0	24	Mês	125,00	150	17.403,57	200	22.631,69	250	27.590,96	300	32.291,48	350	36.743,01	32.291,48	774.995,52	
	68	Roteador Internet - Sede 2	0	24	Mês	2.290,00	-	-	-	-	-	-	-	-	-	-	2.290,00	54.960,00	
	69	Implantação Solução - Lote 2	1	1	Implantação	2.000,00	-	-	-	-	-	-	-	-	-	-	2.000,00	2.000,00	
	70	Repasse de Conhecimento - Roteador Internet - Sede 2	0	1	Turma	5.000,00	-	-	-	-	-	-	-	-	-	-	5.000,00	5.000,00	
Valor total estimado																		**9.401.102,24**	

* O valor de referência é igual ao valor unitário exceto para os itens que são aplicáveis o cálculo de faixas (itens 1 a 27, 29 a 55, 61 e 67), nestes casos o valor de referência é o valor praticado para a faixa 4.

Tabela 7 – Preços estimados

21. Considerando os preços praticados no mercado, a aquisição está estimada em R$ 9.401.102,24 (nove milhões, quatrocentos e um mil, cento e dois reais e vinte e quatro centavos).

22. DOS ANEXOS

22.1. Constituem-se anexos deste Termo de Referência:

22.1.1. ANEXO I – ESPECIFICAÇÃO TÉCNICA;

22.1.2. ANEXO II - DEFINIÇÃO DOS NÍVEIS MÍNIMOS DE SERVIÇO;

22.1.3. ANEXO III - ESPECIFICAÇÃO DOS SERVIÇOS DE TRANSFERENCIA DE CONHECIMENTO;

22.1.4. ANEXO IV - MODELOS DOS DOCUMENTOS DE HABILITAÇÃO;

22.1.5. ANEXO V - MINUTA DO TERMO DE CONFIDENCIALIDADE

22.1.6. ANEXO VI - TERMO DE RESPONSABILIDADE E SIGILO

22.1.7. ANEXO VII - ENDEREÇOS DA MINISTÉRIO DA TRANSPARÊNCIA, FISCALIZAÇÃO E CONTROLADORIA-GERAL DA UNIÃO

22.1.8. ANEXO VIII - MODELO DA PROPOSTA DE PREÇOS;

Brasília-DF, de maio de 2018.

GUSTAVO MOURA DE SOUSA
Integrante Requisitante e Técnico
[ASSINATURA ELETRÔNICA]

BIANCA CRISTINA LESSA ENDERS
Integrante Administrativo
[ASSINATURA ELETRÔNICA]

GUSTAVO TOMÁS COSTA
Gerente de Projetos
[ASSINATURA ELETRÔNICA]

Considerando a importância da solução de TI a ser contratada para as atividades da Casa e em face das justificativas apresentadas, aprovo o presente documento.

ANTONIO MAROYSIO DOS SANTOS CARNEIRO

Coordenador-Geral de Infraestrutura Tecnológica

[ASSINATURA ELETRÔNICA]

ANEXO I DO TERMO DE REFERÊNCIA

ESPECIFICAÇÃO TÉCNICA

Observações:

1) Todos os requisitos especificados, independentemente do verbo utilizado, deverão estar habilitados e completamente funcionais, exceto quando explicitamente mencionado o contrário;

2) A licitante deverá apresentar, para cada um dos requisitos especificados, uma comprovação de que a solução proposta atende ao requisito. Esta comprovação deverá ser feita por meio da indicação do documento público (eletrônico ou impresso) e da numeração da página (ou localização no texto) onde a equipe técnica da CGU possa confirmar tais argumentos. Na Tabela 1 deverá ser especificado o documento, e na coluna **COMPROVAÇÃO** das especificações deverá ser especificado o **ÍNDICE** do documento na Tabela 1 e a **NUMERAÇÃO DA PÁGINA** (ou localização no texto do documento) para comprovação;

3) A CGU reserva-se o direito de diligenciar, após apresentação da proposta, o fornecedor e/ou fabricante para comprovação das informações prestadas na proposta e nas tabelas.

4) A documentação de comprovação de atendimentos aos requisitos poderá ser apresentada em língua inglesa.

Tabela 1

ÍNDICE	DOCUMENTO (anexo impresso ou sítio da internet)
A	
B	
C	
D	
E	
F	
G	
H	
I	
J	

A solução ofertada deve atender a <u>todos</u> os requisitos técnicos descritos abaixo:

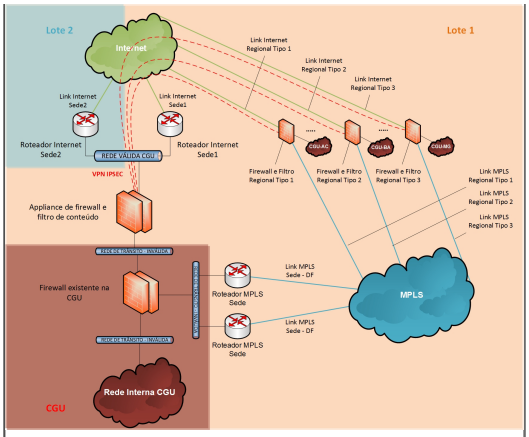
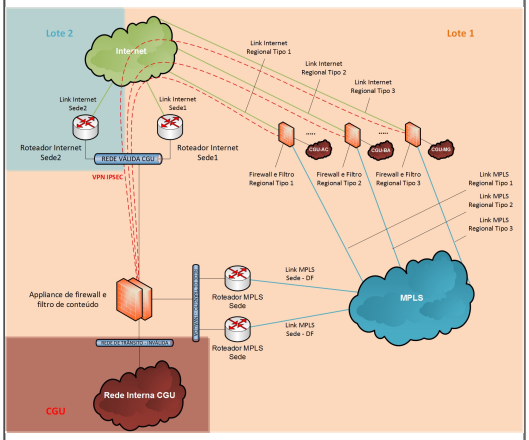
Termo	Significado
ACL	Access Control List
AS (plural ASes)	Autonomous System
BGP	Border Gateway Protocol
CoS	Class of Service
CPE	Customer Premises Equipment
CDN	Content Deliveryt Network
DIO	Distribuidor Interno Óptico
DSCP	Differentiated Services Code Point
IKE	Internet Key Exchange
FIB	Forwarding Information Base
HUB-AND-SPOKE	Topologia em estrela, em que o nó central é chamado de HUB e as extremidades são chamadas de SPOKES
IPS	Intrusion Prevention System
IXP	Internet Exchange Point
MP-BGP	Multiprotocol Border Gateway Protocol
NAT	Network Address Translation
NTP	Network Time Protocol
PE	Provider Equipment
PIM	Protocol Independent Multicast
POD	Point of Delivery
POP	Point of Presence
QoS	Quality of Service
RSSO	Radius Single Sign-On
SSL	Secure Socket Layer
UTP	Unshielded Twisted Pair
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WRED	Weighted Random Early Detection

ITEM / SUBITEM	ESPECIFICAÇÃO	COMPROVAÇÃO (ÍNDICE E PÁGINA)
1.	**Características gerais e premissas aplicáveis a todos os itens**	-
1.1.	**Funcionamento geral da solução**	-
1.1.1.	• A CONTRATANTE pretende implementar uma solução de	-

	comunicação entre suas unidades, bem como de suas unidades com a rede mundial de computadores (Internet).	
1.1.2.	• A sede da CONTRATANTE está localizada em Brasília, enquanto as unidades regionais estão nas capitais de todos os estados brasileiros.	-
1.1.3.	• O objetivo é que exista uma rede MPLS para a comunicação entre todas as unidades. Adicionalmente, cada localidade deve ter conexão direta com a Internet.	-
1.1.4.	• Em situações normais, os tráfegos de sistemas e serviços corporativos, além dos tráfegos multimídia de telefonia IP e videoconferência devem ser encaminhados exclusivamente pela rede MPLS. Por outro lado, os serviços que estiverem publicados na Internet devem ser acessados diretamente sem a necessidade de utilização da rede MPLS.	-
1.1.5.	• Em situações de falha da rede MPLS, alternativamente os tráfegos corporativos devem ser encaminhados entre as regionais da CONTRATANTE e a sede utilizando túneis VPN IPSEC que devem ser estabelecidos pela Internet. Os túneis VPN devem utilizar a topologia hub-and-spoke, com centralização nos equipamentos da sede.	-
1.1.6.	• Em situações de falha dos Links de internet das unidades regionais, o tráfego deve ser encaminhado pela rede MPLS até a sede em Brasília para que então possa ser enviado para a Internet.	-
1.1.7.	• A configuração do encaminhamento do tráfego e da contingência em casos de falha deve ser feita preferencialmente com a correta configuração do protocolo de roteamento OSPF, embora seja permitida a utilização de tecnologias SDN-WAN em que o encaminhamento de tráfego é feito com base no perfil de tráfego em vez da utilização de rotas (situação em que a topologia poderá ser revista). Também será permitida a redistribuição de rotas entre o OSPF e outros protocolos de roteamento. O OSPF deve ser utilizado para efetuar a troca de informações de roteamento com o equipamento denominado "Firewall existente na CONTRATANTE".	-
1.1.8.	• Objetivando redundância e independência das conexões à Internet e dos serviços de proteção, os lotes 1 e 2 deverão ser arrematados por fornecedores distintos, sendo vedado o compartilhamento de serviços ou de infraestrutura em qualquer nível.	-
1.2.	**Características gerais dos links MPLS e Internet**	-
1.2.1.	• As unidades regionais da CONTRATANTE farão acesso à Internet, mas não haverá nenhum serviço publicado externamente. Em função do exposto, basta que seja fornecido pela CONTRATADA 1 (um) IPv4 válido para os links internet dessas localidades. Será permitida a utilização da RFC 3021 (utilização de prefixos /31 IPv4 em links ponto-a-ponto) nesses casos.	-
1.2.2.	• Devem transportar pacotes IPv4 e IPv6 com 1500 (mil e quinhentos) bytes sem exigir a fragmentação dos mesmos na camada 3 do modelo OSI.	-
1.2.3.	• Os links devem suportar IPv6, não sendo necessário o fornecimento de endereçamento para as redes internas da CONTRATANTE.	-
1.2.4.	• A velocidade de todos os Links deverá ser simétrica e disponível de forma simultânea, ou seja, mesma velocidade de entrada e de saída (Links full-duplex).	-
1.2.5.	• Todos os canais deverão ser entregues e mantidos sem nenhum mecanismo de restrição a qualquer volume de tráfego.	-
1.2.6.	• Para as unidades regionais, a CONTRATADA poderá entregar os links MPLS e Internet diretamente nos appliances de Firewall/Filtro de Conteúdo ou poderá opcionalmente utilizar roteadores específicos para interconectar cada um dos links. Caso seja feita opção por utilizar roteadores, não poderá haver custo adicional para tais equipamentos e todos os demais requisitos para a utilização da solução devem ser mantidos e respeitados.	-
1.3.	**Regime de operação dos serviços**	-
1.3.1.	• Regime de operação de todos os serviços deverá ser de 24 (vinte e quatro) horas por dia, durante os 7 (sete) dias da	-

	semana.	
1.3.2.	• Eventuais manutenções preventivas dos serviços deverão ser agendadas com antecedência mínima de 5 (cinco) dias corridos.	-
1.4.	**Última milha**	-
1.4.1.	• A última milha caracteriza-se como o meio de comunicação utilizado para interligar cada unidade da CONTRATANTE ao backbone da CONTRATADA.	-
1.4.2.	• Deverão ser utilizados Links de comunicação terrestre confeccionados com fibra óptica. Apenas será permitida a conversão do meio óptico para UTP para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances de firewall/filtro de conteúdo.	-
1.4.3.	• A CONTRATADA se responsabilizará pela implantação, nas unidades da CONTRATANTE, de toda a infraestrutura necessária à configuração dos canais de comunicação. Dentre os itens de infraestrutura a serem fornecidos pela CONTRATADA, caso seja necessário, estão: construção/reforma de caixas de passagem, instalação de dutos entre a caixa de passagem e a unidade da CGU, lançamento de cabos, e recomposição de calçada quando for necessário. Não estão incluídas neste item obras internas nas unidades da CGU, como lançamento de canaletas e recomposição de gesso.	-
1.5.	**Dupla abordagem:**	-
1.5.1.	• Para as unidades regionais da CONTRATANTE, o link MPLS e o link internet deverão ser entregues com dupla abordagem em fibra óptica. O mesmo requisito deve ser respeitado para os dois links MPLS da sede. Nas duas situações descritas acima, os links poderão ser atendidos pelo mesmo POP da CONTRATADA.	-
1.5.2.	• Os circuitos com dupla abordagem não poderão ser instalados no mesmo PE. O circuito do item 61 também não poderá compartilhar o PE com nenhum dos dois circuitos do item 27.	-
1.5.3.	• Os links com dupla abordagem, em fibra óptica, que devem ser estabelecidas por caminhos completamente distintos, não devendo haver nenhum ponto de falha comum entre os dois links de comunicação. Por ponto de falha comum entende-se:	-
1.5.4.	◦ Utilização compartilhada dos mesmos equipamentos no ambiente da CONTRATADA ou em ambientes públicos: roteadores, multiplexadores, switches, conversores ópticos e outros. Para os links das unidades regionais da CONTRATANTE (não se aplica aos links da sede) será permitido o compartilhamento de equipamentos dentro das instalações da CONTRATANTE apenas;	-
1.5.5.	◦ Utilização compartilhada de Links fisicos ou lógicos no ambiente da CONTRATADA ou em ambientes públicos, como: utilização dos mesmos encaminhamentos, dutos, caixas de passagem, DIOs e outros. Para os links das unidades regionais da CONTRATANTE (não se aplica aos links da sede) será permitido o compartilhamento da caixa de passagem (na calçada do prédio da CONTRATANTE) e dos dutos da caixa de passagem até o rack dentro das instalações da CONTRATANTE apenas.	-
1.6.	**Fornecimento de energia e disponibilização de espaço**	-
1.6.1.	• Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação, se necessário. Caso seja necessário devem ser fornecidos adaptadores para racks ou bandejas.	-
1.6.2.	• A CONTRATANTE disponibilizará circuitos elétricos e até 8 Us (oito unidades de rack) em bastidor de 19" para acomodar os equipamentos da CONTRADADA em suas unidades regionais.	-
1.6.3.	• A CONTRATANTE disponibilizará circuitos elétricos redundantes e a CONTRATADA deverá providenciar 1 (um) rack de 19" com dimensões adequadas para acomodar os equipamentos na sede em Brasília.	-
1.7.	**Características comuns aos equipamentos e gerência**	-
1.7.1.	• Os equipamentos deverão ser dimensionados, fornecidos, instalados e configurados, pela CONTRATADA, garantindo-se	-

	o desempenho e os níveis de serviços contratados.	
1.7.2.	• A CONTRATANTE deverá ter acesso do tipo leitura nos equipamentos "roteador internet" e "roteador MPLS" da sede e das regionais (caso sejam instalados).	-
1.7.3.	• A CONTRATANTE deverá ter acesso do tipo escrita nos equipamentos denominados "appliance de firewall/filtro de conteúdo". A CONTRATANTE isentará a CONTRADATA de incidentes causados por erros de configuração causados pela própria CONTRATANTE. A CONTRATADA poderá ter acesso do tipo leitura nos referidos equipamentos.	-
1.7.4.	• A qualquer momento durante a execução do contrato, a CONTRATANTE poderá optar por solicitar o acesso do tipo escrita para os equipamentos "roteador internet" da sede, por utilizarem o ASN e o bloco de endereços da CGU. Nesta situação, a CONTRATADA poderá ter acesso do tipo leitura nos referidos equipamentos.	-
1.7.5.	• Por acesso entende-se permissão de ingresso utilizando interface web utilizando https, linha de comando utilizando ssh, possibilidade de obtenção de dados via SNMP e syslog.	
1.7.6.	• Mesmo para as situações em que a CONTRATANTE possuir acesso de escrita, a CONTRATADA não estará isenta de oferecer suporte para qualquer necessidade em que seja necessário acionar o fabricante, bem como em casos de indisponibilidade, substituição do hardware ou partes dos hardwares, atualização do firmware entre outras possíveis situações. A CONTRATANTE não acionará a CONTRATADA para configurações básicas e rotineiras, como: configurações de interfaces, regras de firewalls e controle de aplicações, ACLs, NATs, SNMP, NTP, VPN client do site, entre outras possíveis situações.	-
1.7.7.	• Todos os equipamentos e links devem suportar tanto IPv4 quanto IPv6, sendo que este último deve estar implementado de forma nativa em pilha dupla.	-
1.7.8.	• Deverão suportar o respectivo tráfego da banda completamente ocupada sem degradação do desempenho, atendendo aos níveis de serviço pretendidos. Para isso deverão apresentar configuração de memória, de CPU e capacidade de vazão compatíveis (de forma qualitativa e quantitativa) com as características e componentes desta especificação.	-
1.7.9.	• Deverão possuir fonte de alimentação com chaveamento automático de tensão de entrada 110/220 VAC a 60 Hz.	-
1.7.10.	• Os appliances de firewall/filtro de conteúdo da sede e de todas as regionais devem ser do mesmo fabricante para que a solução de gerência seja única e as configurações possam ser aplicadas em todos os dispositivos de forma unificada.	-
1.8.	**Topologia da solução**	-
1.8.1.	• As regionais da CONTRATANTE foram divididas em 3 tipos conforme a quantidade de pessoas e a capacidade de seus links. Esses parâmetros serão utilizados para detalhar as capacidades dos appliances de firewall/filtro de conteúdo. Apenas para referência, as unidades regionais tipo 1 possuem até 70 (setenta) usuários simultâneos, as unidades regionais tipo 2 possuem até 100 (cem) usuários simultâneos, as unidades tipo 3 possuem até 150 (cento e cinquenta) usuários simultâneos e a sede possui até 2.000 (dois mil) usuários simultâneos.	-
1.8.2.	• Foi elaborada uma topologia lógica da solução. O diagrama também detalha a distribuição dos itens em função dos lotes. Para simplificar o diagrama foram demonstradas apenas 3 unidades regionais da CONTRATANTE (uma de cada tipo).	-
1.8.3.		-

		
1.8.4.	• A CONTRATANTE poderá desativar o cluster de equipamentos denominado “Firewall existente na CONTRATANTE” e migrar todas as conexões e regras para os equipamentos denominados “appliances de firewall/filtro de conteúdo da sede”. Para isso as especificações do referido item irão prever interfaces e throughput adequados. Neste caso a topologia lógica da solução será modificada para a forma como está descrita no diagrama abaixo. Para simplificar o desenho há alguns segmentos não representados na topologia (em especial nos firewalls da sede), mas a quantidade de portas do “appliances de firewall/filtro de conteúdo da sede” comporta os segmentos em questão.	-
1.8.5.		-
1.8.6.	• Não será necessário fornecer nenhum switch para o atendimento da solução proposta. Os barramentos ethernet representados nas topologias lógicas serão de responsabilidade da CONTRATANTE.	-
1.8.7.	• A CONTRATANTE poderá utilizar os roteadores internet (itens 62 e 68) para interconexão a qualquer IXP.	-
2.	**Características comuns dos itens 1 a 27 - Link MPLS**	-
2.1.	**Backbone**	-
2.1.1.	• Rede de dados com capacidade de encaminhar pacotes IPv4 e IPv6, composto por uma malha de canais de comunicação dedicados, que permitirá a conexão entre todas as unidades da CONTRATANTE sob uma topologia any-to any (full mesh).	-
2.1.2.	• Deve permitir o isolamento total do tráfego e das tabelas de roteamento da CONTRATANTE e dos demais clientes da CONTRATADA utilizando tecnologia de VRFs criando uma VPN MPLS. Em função disso a CONTRATANTE poderá utilizar qualquer faixa de endereço privados IPv4 em sua estrutura de rede.	-
2.1.3.	• Deverá possuir capacidade de tráfego em IP multicast para que aplicações de voz e vídeo que utilizem esta tecnologia possam ser implementadas independente de qualquer configuração no backbone. Não será permitido o estabelecimento de túneis entre os roteadores para que o tráfego multicast seja encaminhado.	-
2.1.4.	• Não serão permitidos POPs atendidos de forma primária por Links de satélite.	-
2.1.5.	• O backbone MPLS deve pertencer inteiramente a ASes do	-

	mesmo grupo econômico.	
2.2.	**Qualidade de Serviço**	-
2.2.1.	• A solução da CONTRATADA deverá suportar a arquitetura Diffserv, incluindo Diffserv sobre redes MPLS.	-
2.2.2.	• De acordo com as prioridades e níveis de serviços definidos, os diferentes tipos de tráfego que serão encaminhados pela Rede CONTRATANTE deverão ser classificados em 5 (cinco) classes de serviços (Diffserv) pela rede MPLS da CONTRATADA, conforme descrito a seguir:	-
2.2.3.	◦ **Voz:** aplicações de voz sensíveis a retardo (delay) e variações de retardo (jitter), que exijam priorização absoluta de tráfego e reserva de banda;	-
2.2.4.	◦ **Vídeo:** aplicações multimídia sensíveis a retardo (delay) e variações de retardo (jitter), que exijam priorização de tráfego e reserva de banda;	-
2.2.5.	◦ **Serviços críticos:** aplicações críticas para o negócio, que exigem entrega garantida, reserva de banda e tratamento prioritário;	-
2.2.6.	◦ **Serviços interativos:** aplicações interativas, que exigem entrega garantida, reserva de banda e tratamento prioritário. Esta classe deve acomodar o tráfego utilizado para medir o SLA;	-
2.2.7.	◦ **Serviços não prioritários:** aplicações com mensagens de tamanho muito variado e não imprescindíveis para o atendimento imediato aos clientes.	-
2.2.8.	• A marcação da classe de serviço dos pacotes deve ser feita pela CONTRATADA utilizando o campo DSCP dos pacotes IP nos CPEs, ou seja, roteadores ou appliances de firewall/filtro de conteúdo.	-
2.2.9.	• As classes podem ser remapeadas quando os pacotes forem encaminhados para o backbone MPLS.	-
2.2.10.	• A CONTRADATA poderá implementar outras classes além das utilizadas pela CONTRATANTE para fins de operação dos protocolos de roteamento e/ou de gerência. As bandas das classes somadas poderão consumir até 2% (dois por cento) da capacidade do link. Caso haja sobreposição de tráfego entre as classes será feita a diferenciação das regras da CONTRATANTE em relação às da CONTRATADA com base em endereços IP de origem e/ou de destino.	-
2.2.11.	• O mapeamento dos tráfegos e larguras de banda de cada classe será definido pela CONTRATANTE, respeitado os seguintes critérios:	-
2.2.12.	◦ A soma das bandas das classes da CONTRATANTE com as classes da CONTRATADA não excederão 97% (noventa e sete por cento) da capacidade do link.	-
2.2.13.	◦ A soma das bandas das classes de **voz** e **vídeo** somadas não excederão 50% (cinquenta por cento) da capacidade do link.	-
3.	**Características específicas dos itens 1 a 16 - Link MPLS - Regionais Tipo 1**	-
3.1.	**A taxa de transmissão deve variar conforme os valores abaixo descritos:**	-
3.1.1.	• 4 Mbps (quatro megabits por segundo);	-
3.1.2.	• 6 Mbps (seis megabits por segundo);	-
3.1.3.	• 8 Mbps (oito megabits por segundo);	-
3.1.4.	• 10 Mbps (dez megabits por segundo);	-
3.1.5.	• 12 Mbps (doze megabits por segundo);	-
4.	**Características específicas dos itens 17 a 23 - Link MPLS - Regionais Tipo 2**	-

4.1.	**A taxa de transmissão deve variar conforme os valores abaixo descritos:**	-
4.1.1.	• 6 Mbps (seis megabits por segundo);	-
4.1.2.	• 8 Mbps (oito megabits por segundo);	-
4.1.3.	• 10 Mbps (dez megabits por segundo);	-
4.1.4.	• 12 Mbps (doze megabits por segundo);	-
4.1.5.	• 14 Mbps (quatorze megabits por segundo);	-
5.	**Características específicas dos itens 24 a 26 - Link MPLS - Regionais Tipo 3**	-
5.1.	**A taxa de transmissão deve variar conforme os valores abaixo descritos:**	-
5.1.1.	• 8 Mbps (oito megabits por segundo);	-
5.1.2.	• 10 Mbps (dez megabits por segundo);	-
5.1.3.	• 12 Mbps (doze megabits por segundo);	-
5.1.4.	• 14 Mbps (quatorze megabits por segundo);	-
5.1.5.	• 16 Mbps (dezesseis megabits por segundo);	-
6.	**Características específicas do item 27 - Link MPLS - Sede – DF**	-
6.1.	**A taxa de transmissão deve variar conforme os valores abaixo descritos:**	-
6.1.1.	• 50 Mbps (cinquenta megabits por segundo);	-
6.1.2.	• 100 Mbps (cem megabits por segundo);	-
6.1.3.	• 150 Mbps (cento e cinquenta megabits por segundo);	-
6.1.4.	• 200 Mbps (duzentos megabits por segundo);	-
6.1.5.	• 250 Mbps (duzentos e cinquenta megabits por segundo).	-
7.	**Item 28 - Roteador MPLS - Sede**	-
7.1.	As características abaixo se referem a 1 (uma) unidade do roteador.	-
7.2.	Além das interfaces utilizadas para o link MPLS e back-to-back (caso seja necessário) deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T, que serão utilizadas na rede interna da CONTRATANTE.	
7.3.	Deve ter no mínimo 2 (duas) fontes de alimentação.	
7.4.	**Devem suportar os seguintes protocolos/funcionalidades:**	-
7.4.1.	• O serviço deve permitir a administração remota, protegida por autenticação usuário/senha e utilizando pelo menos os protocolos SSHv2 e HTTPS;	
7.4.2.	• Priorização e conformação de tráfego com pelo menos os seguintes métodos: Traffic Policing, Traffic Shaping, Class Based Weighted Fair Queueing, Low-latency Queuing;	
7.4.3.	• WRED;	
7.4.4.	• Implementar classificação de tráfego com base em ACLs, no campo DSCP e no campo CoS;	
7.4.5.	• Implementar a marcação e priorização do tráfego previamente classificado com base no campo DSCP e no campo CoS;	

7.4.6.	• Roteamento IP Multicast através do protocolo PIM nas versões 1 e 2 e nos modos Sparse Mode e Dense Mode;	
7.4.7.	• Implementar RFC 3768 VRRP.	
7.4.8.	• OSPFv2 e OSPFv3 com suporte a autenticação de vizinhança utilizando protocolo MD5;	
7.4.9.	• Cliente NTP, contemplando suporte à autenticação entre os peers, conforme definido na RFC 1305. Deve possibilitar a especificação da interface de origem dos pacotes NTP;	
7.4.10.	• Agente SNMP nas versões 2c e 3, com suporte a MIB-II, possibilitando acesso de leitura com restrição dos endereços que podem efetuar consultas SNMP;	
7.4.11.	• Capacidade de geração e armazenamento de logs locais;	
7.4.12.	• Protocolo Syslog com a possibilidade de envio de timestamp baseado no relógio do roteador;	
7.4.13.	• Protocolo IP SLA ou similar, ou sejam deve ser capaz de responder a pacotes de simulação de tráfegos. Devem ser suportados, no mínimo, os protocolos ICMP, TCP e UDP. Os dados referentes aos tráfegos simulados devem ser disponibilizados via SNMP;	
7.4.14.	• Implementar ACLs com pelo menos os seguintes parâmetros;	
7.4.15.	◦ Endereços IP de host ou rede, de pacotes IPv4 e IPv6 (tanto de origem quanto de destino);	
7.4.16.	◦ Tipos de pacote ICMP;	
7.4.17.	◦ Portas e faixas de portas dos protocolos TCP e UDP (tanto de origem quanto de destino);	
7.4.18.	◦ Deve permitir criar regras com base em hora do dia e com base nos dias da semana;	
7.4.19.	• Protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow, IPFIX ou similar, contemplando no mínimo as seguintes informações:	
7.4.20.	◦ IP de origem/destino;	
7.4.21.	◦ Parâmetro “protocol type” do cabeçalho IP;	
7.4.22.	◦ Porta TCP/UDP de origem/destino;	
7.4.23.	◦ Campo TOS ou DSCP do cabeçalho IP;	
7.4.24.	◦ Interface do equipamento em que o tráfego foi identificado;	
7.4.25.	◦ A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo padrão de mercado para este fim;	
8.	**Características comuns dos itens 29 a 54, 61 e 67 - Link Internet**	-
8.1.	Acessos IP permanentes que possibilitem a interligação (IPv4 e IPv6) das unidades da CONTRATANTE à rede mundial de computadores, Internet.	-
8.2.	O backbone da CONTRATADA deverá possuir conexão direta com pelo menos 1 (um) IXP para troca de trânsito.	
8.3.	O backbone da CONTRATADA deverá possuir pelo menos 2 (duas) saídas internacionais próprias, ou contratados para seu uso.	
8.4.	O backbone da CONTRATADA deverá possuir interligação direta através de canais próprios e dedicados, a pelo menos 3 (três) outros ASes (além das conexões descritas no item anterior), com peering BGP IPv4 e IPv6. As bandas de saída entre referidos ASes deverão somar pelo menos 10 Gbps (dez gigabits por segundo).	
8.5.	Disponibilizar serviço de DNS da CONTRATADA, capaz de resolver direta e reversa endereços IPv4 e IPv6 de internet.	-

8.6.	Não será permitido o uso de tecnologias DSL, BLC Cable, 3G e 4G.	-
8.7.	Todos os links internet das regionais e o PE que atenderá o link internet (Item 61) devem necessariamente pertencer a ASes do mesmo grupo econômico para que a latência da VPN seja reduzida. Por esse motivo o referido item deve ser licitado em conjunto com os demais itens do lote 1.	
9.	**Características específicas dos itens 29 a 44 - Link Internet - Regionais Tipo 1**	-
9.1.	**A taxa de transmissão deve variar conforme os valores abaixo descritos:**	-
9.1.1.	• 6 Mbps (seis megabits por segundo);	-
9.1.2.	• 10 Mbps (dez megabits por segundo);	-
9.1.3.	• 14 Mbps (quatorze megabits por segundo);	-
9.1.4.	• 18 Mbps (dezoito megabits por segundo);	-
9.1.5.	• 22 Mbps (vinte e dois megabits por segundo);	-
10.	**Características específicas dos itens 45 a 51 - Link Internet - Regionais Tipo 2**	-
10.1.	**A taxa de transmissão deve variar conforme os valores abaixo descritos:**	-
10.1.1.	• 8 Mbps (oito megabits por segundo);	-
10.1.2.	• 12 Mbps (doze megabits por segundo);	-
10.1.3.	• 16 Mbps (dezesseis megabits por segundo);	-
10.1.4.	• 20 Mbps (vinte megabits por segundo);	-
10.1.5.	• 24 Mbps (vinte e quatro megabits por segundo);	-
11.	**Características específicas dos itens 52 a 54 - Link Internet - Regionais Tipo 3**	-
11.1.	**A taxa de transmissão deve variar conforme os valores abaixo descritos:**	-
11.1.1.	• 10 Mbps (dez megabits por segundo);	-
11.1.2.	• 14 Mbps (quatorze megabits por segundo);	-
11.1.3.	• 18 Mbps (dezoito megabits por segundo);	-
11.1.4.	• 22 Mbps (vinte e dois megabits por segundo);	-
11.1.5.	• 26 Mbps (vinte e seis megabits por segundo);	-
12.	**Características comuns dos itens 55 a 58 - Appliance de Firewall/Filtro de Conteúdo**	-
12.1.	Aplliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW). Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.	-
12.2.	A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.	
12.3.	Deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.	
12.4.	Nos estados, caso a CONTRATADA opte por fornecer CPEs para o link MPLS e/ou para o link internet, as características do conjunto formado pelos três equipamentos devem atender aos requisitos deste item.	

12.5.	Deve implementar funcionalidade de anti-spoofing, configurável por segmento de rede de modo que seja possível: utilizar o próprio endereçamento da interface ou especificar quais redes serão utilizadas como referência para permitir/negar o ingresso de um pacote.	
12.6.	Deve permitir a configuração de ISP (rota default estática) com a utilização de probe para verificar a disponibilidade do provedor. A probe deve permitir verificar o acesso HTTP a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha (ou alta latência).	
12.7.	As funcionalidades de controle de aplicações, filtro de URLs, VPN IPSec e SSL, QoS, SSL Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas durante toda a vigência do contrato.	
12.8.	**Deve possuir pelo menos as seguintes funcionalidades:**	-
12.8.1.	• Policy based routing ou policy based forwarding;	
12.8.2.	• Jumbo Frames;	
12.8.3.	• DHCP Relay;	
12.8.4.	• Suportar IGMP, v2 e v3;	
12.8.5.	• O serviço deve permitir a administração remota, protegida por autenticação usuário/senha e utilizando pelo menos os protocolos SSHv2 e HTTPS;	
12.8.6.	• Roteamento IP Multicast através do protocolo PIM nas versões 1 e 2 e nos modos Sparse Mode e Dense Mode (não será exigida a implementação dos dois modos de forma simultânea);	
12.8.7.	• OSPFv2 e OSPFv3 com suporte a autenticação de vizinhança utilizando protocolo MD5;	
12.8.8.	• Cliente NTP, contemplando suporte à autenticação entre os peers;	
12.8.9.	• Agente SNMP nas versões 2c e 3, com suporte a MIB-II, possibilitando acesso de leitura com restrição dos endereços que podem efetuar consultas SNMP;	
12.8.10.	• Protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow, sFlow, IPFIX ou similar, contemplando no mínimo as seguintes informações:	
12.8.11.	◦ IP de origem/destino;	
12.8.12.	◦ Parâmetro “protocol type” do cabeçalho IP;	
12.8.13.	◦ Porta TCP/UDP de origem/destino;	
12.8.14.	◦ Interface do equipamento em que o tráfego foi identificado.	
12.9.	**Deve suportar os seguintes tipos de NAT:**	-
12.9.1.	• NAT dinâmico (Many-to-1);	
12.9.2.	• NAT dinâmico (Many-to-Many);	
12.9.3.	• NAT estático (1-to-1);	
12.9.4.	• NAT estático (Many-to-Many);	
12.9.5.	• NAT estático bidirecional 1-to-1;	
12.9.6.	• Tradução de porta (PAT);	
12.9.7.	• NAT de origem;	
12.9.8.	• NAT de destino;	
12.9.9.	• NAT de origem e NAT de destino simultaneamente.	

12.10.	**Controle de política de firewall**	-
12.10.1.	• Controles de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;	
12.10.2.	• Controle, inspeção e decriptografia de SSL por política para trafego de entrada (inbound) e Saída (outbound);	
12.10.3.	• Deve suportar offload de certificado em inspeção de conexões SSL de entrada (inbound);	
12.10.4.	• Deve permitir bloquear, pelo menos, os seguintes tipos de arquivos ou extensões: bat, cab, dll, exe, pif, e reg;	
12.10.5.	• Suporte a objetos e regras multicast;	
12.10.6.	• Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;	
12.10.7.	• Suportar a criação de políticas com data de expiração.	
12.11.	**Controle de aplicações**	-
12.11.1.	• Deve possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;	
12.11.2.	• Deve ser possível a liberação e bloqueio somente das aplicações sem a necessidade de liberação de portas e protocolos;	
12.11.3.	• Reconhecer diversas aplicações diferentes, incluindo, mas não limitado: peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, audio, vídeo, proxy, mensageria instantânea, compartilhamento de arquivos, e-mail;	
12.11.4.	• 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;	
12.11.5.	• Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam comunicações criptografadas, tais como Skype e ataques utilizando a porta 443;	
12.11.6.	• Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;	
12.11.7.	• Deve ser possível a liberação e bloqueio das aplicações (ou de suas funcionalidades) por usuário, grupo de usuários, endereço IP ou rede específica;	
12.11.8.	• Atualizar a base de assinaturas de aplicações automaticamente;	
12.11.9.	• Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;	
12.11.10.	• O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;	
12.11.11.	• Deve alertar o usuário quando uma aplicação for bloqueada;	
12.11.12.	• Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat mas bloquear a transferência de arquivos, permitir acesso ao Facebook mas bloquear a visualização de vídeos, permitir acesso ao whatsapp mas bloquear a transferência de arquivos.	
12.11.13.	• Deve possibilitar a diferenciação de aplicações Proxies	

	(ghostsurf, freegate, ultrasurf, tor, etc) possuindo granularidade de controle/políticas para os mesmos;	
12.11.14.	• Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:	
12.11.14.1.	• Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc);	
12.11.14.2.	• Nível de risco da aplicação;	
12.11.14.3.	• Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.	
12.12.	**Prevenção de ameaças**	-
12.12.1.	• Deve possuir módulo de IPS integrado no próprio appliances,	
12.12.2.	• Deve incluir assinaturas de prevenção de intrusão (IPS);	
12.12.3.	• Deve-se sincronizar as assinaturas de IPS quando implementado em alta disponibilidade ativo/ativo e ativo/passivo (quando aplicável);	
12.12.4.	• Deverá possuir os seguintes mecanismos de inspeção de IPS:	-
12.12.4.1.	◦ Análise de padrões de estado de conexões;	
12.12.4.2.	◦ Análise de decodificação de protocolo;	
12.12.4.3.	◦ Análise para detecção de anomalias de protocolo;	
12.12.4.4.	◦ IP Defragmentation;	
12.12.4.5.	◦ Remontagem de pacotes TCP;	
12.12.4.6.	◦ Bloqueio de pacotes malformados;	
12.12.5.	• Ser capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;	
12.12.6.	• Detectar e bloquear a origem de port scans;	
12.12.7.	• Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;	
12.12.8.	• Possuir assinaturas para bloqueio de ataques de buffer overflow;	
12.12.9.	• Deverá possibilitar a criação de assinaturas customizadas;	
12.12.10.	• Suportar bloqueio de arquivos por tipo;	
12.12.11.	• Identificar e bloquear comunicação com botnets;	
12.12.12.	• Deve suportar várias técnicas de prevenção, incluindo Drop (Cliente, Servidor e ambos);	
12.12.13.	• Deve suportar referência cruzada com CVE (Common Vulnerabilities and Exposures);	
12.12.14.	• Deve suportar a captura de pacotes (PCAP), por assinatura de IPS;	
12.12.15.	• Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;	
12.12.16.	• Proteção contra downloads involuntários usando HTTP ou HTTPS de arquivos executáveis;	
12.12.17.	• Rastreamento de vírus em pdf;	

12.12.18.	• Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate, como: zip e gzip;	
12.12.19.	• Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall, considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;	
12.12.20.	• Deve permitir a inspeção de arquivos incorporados em outros arquivos ou arquivos que tenham sua extensão alterada na tentativa de contornar sua detecção.	
12.13.	**Identificação de usuários**	-
12.13.1.	• Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem (usuários e grupos de usuários) está utilizando quais aplicações através da integração com serviços de diretório, autenticação via Ldap, Microsoft Active Directory e base de dados local;	
12.13.2.	• Suporte a autenticação Kerberos;	
12.13.3.	• Deve possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;	
12.13.4.	• Quando integrado ao Microsoft Active Directory, deve permitir identificar usuários dentro de grupos, mesmo que estejam em um uma hierarquia de grupo dentro de grupo.	
12.13.5.	• Deve possuir suporte a identificação de múltiplos usuários conectados, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão em uso;	
12.13.6.	• Deve permitir a atualização da identificação de um usuário caso este mude de endereço IP e mesmo que mais de um dispositivo esteja sendo utilizado de forma simultânea, evitando a necessidade de que sejam configurados endereços fixos.	
12.14.	**QoS**	-
12.14.1.	• Com a finalidade de controlar aplicações e tráfego, cujo consumo possa ser excessivo (como youtube, ustream, etc) e ter um alto consumo de largura de banda, a solução deve, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por aplicação, tanto de áudio como de vídeo streaming;	
12.14.2.	• Deve suportar a funcionalidade de configurar horários para navegação, permitindo controle por usuário e tempo;	
12.14.3.	• Suportar a criação de políticas de QoS por:	-
12.14.4.	◦ Por usuário e grupo do LDAP/AD;	
12.14.5.	◦ Por aplicações (traffic shaping);	
12.14.6.	◦ Por interface física ou lógica do equipamento;	
12.14.7.	• Suportar priorização de protocolos de voz e video como H.323, SIP, SCCP, MGCP e aplicações como Skype;	
12.14.8.	• Deve suportar conformação de tráfego com pelo menos os seguintes métodos: Traffic Policing e Traffic Shaping;	
12.14.9.	• Deve implementar classificação de tráfego com no campo DSCP;	
12.14.10.	• Implementar a marcação e priorização do tráfego previamente classificado com base no campo DSCP;	
12.15.	**VPN**	-
12.15.1.	• Deve implementar VPN IPSec com capacidade de implementar túneis site-to-site do tipo hub-and-spoke.	

12.15.2.	• Deve permitir o estabelecimento do túnel utilizando uma "chave secreta" ou certificados digitais.	
12.15.3.	• Deve implementar IKEv1 e IKEv2;	
12.15.4.	• Deve oferecer suporte pelo menos aos seguintes algoritmos de criptografia: 3DES, AES-128, AES-192 e AES-256;	
12.15.5.	• Deve oferecer suporte pelo menos aos seguintes algoritmos de autenticação: MD5, SHA-1, SHA-256, SHA-384, SHA-512;	
12.16.	**Filtro de URLs**	-
12.16.1.	• Deve implementar a funcionalidade de filtro de URL HTTP e HTTPS.	
12.16.2.	• Deve implementar a funcionalidade de filtro de conteúdo HTTP.	
12.16.3.	• Deve implementar a funcionalidade de SSL Scanner.	
12.16.4.	• Deve ter funcionalidade de proxy transparente HTTP/HTTPS (situação em que o cliente não precisa encaminhar o tráfego para o IP do proxy e não há instalação de cliente). No modo proxy transparente o cliente acreditar estar acessando diretamente o conteúdo desejado.	
12.16.5.	• Deve implementar a funcionalidade de cache de dados.	
12.16.6.	• Deve bloquear as tentativas de acesso proibidas pela política antes que ocorra o carregamento da página solicitada, exibindo mensagem customizada para o bloqueio.	
12.16.7.	• Deve garantir o monitoramento do tráfego internet independente de plataforma, sistema operacional ou aplicação utilizada pelos usuários.	
12.16.8.	• Não deve instalar nem executar agentes, módulos ou scripts nas estações de trabalho para prover qualquer serviço. Deve ser transparente ao usuário final.	
12.17.	• Controle de acesso à Internet	-
12.17.1.	◦ As regras de acesso à Internet devem se basear tanto na requisição quanto na resposta HTTP;	
12.17.2.	◦ Deve permitir a criação de regras baseadas em horário do dia;	
12.17.3.	◦ Deve possuir controle de downloads/uploads de arquivos pelo nome, tipo ou extensão do arquivo;	
12.17.4.	◦ Deve possuir controle de acesso à Internet por domínio, exemplo: gov.br, org.br;	
12.17.5.	◦ Deve possuir controle de acesso à Internet por categorias de sites web;	
12.17.6.	◦ Deve possuir controle de acesso à Internet por lista de sites web proibidos (blacklist) customizável;	
12.17.7.	◦ Deve possuir controle de acesso à Internet por lista de sites web permitidos (whitelist) customizável;	
12.17.8.	◦ Deve possuir mecanismo automático para detecção e bloqueio em tempo real de tráfego (inbound/outbound) originado por códigos maliciosos tipo malwares ou spywares;	
12.17.9.	◦ O serviço deve possuir mecanismo automático para detecção de tráfego tunelado na porta 80;	
12.17.10.	◦ Deve permitir que as páginas de erro e bloqueio sejam customizáveis;	
12.17.11.	◦ Deve possuir compatibilidade com filtros de busca segura (safe-search filters), oferecidos por sites web de busca;	
12.17.12.	◦ Deve permitir a definição e aplicação das regras por meio de expressões regulares;	

12.17.13.	◦ Deve permitir a liberação/bloqueio de componentes específicos de sites de redes sociais, tais como chat e comentários do site www.facebook.com ou postagem no site www.twitter.com;	
12.18.	• Categorização de sites web	-
12.18.1.	◦ Deve conter base com no mínimo 15 (quinze) milhões de URL ´s cadastradas, e pelo menos 45 (quarenta e cinco) categorias previamente definidas e possibilidade de criação de novas categorias personalizadas;	
12.18.2.	◦ Deve permitir a classificação/categorização de sites de acordo com o assunto;	
12.18.3.	◦ Deve possuir no mínimo as seguintes categorias (ou similares): pornografia, nudez, sites maliciosos, webmail, blog/fotolog, jogos, hacking, racismo, comunidades virtuais, radio e tv, streaming, instant messaging, chat, sites de download, storage online, P2P, medias sociais, sites maliciosos e acesso remoto;	
12.18.4.	◦ Deve possibilitar que URLs não cadastradas possam ser enviadas ao fabricante para a devida categorização;	
12.18.5.	◦ Deve permitir à CONTRATANTE reclassificar, a seu critério, os registros de site web que julgar necessários.	
12.19.	• Atualização da base de sites	-
12.19.1.	◦ Durante o período de prestação do serviço a base de sites web deve ser atualizada automaticamente pela solução, via Internet. A periodicidade de atualização deve ser customizável. Essa atualização pode ser feita pela Solução de Gerência dos e Appliances de Firewall/Filtro de Conteúdo;	
12.19.2.	◦ A atualização da base de sites web deve transcorrer de forma transparente, sem comprometer a execução dos serviços;	
12.19.3.	◦ A ausência de atualização da base de sites web, por qualquer motivo, não deve interromper nem comprometer funcionalidades da solução;	
12.19.4.	◦ Durante o período de prestação do serviço, os sites web devem ser atualizados, sempre na categoria que reflita o seu conteúdo mais recente, ou seja, em caso de modificação, deve ser reclassificado para a categoria pertinente;	
12.19.5.	◦ Durante o período de prestação do serviço, sites web de phishing, spyware ou que tenham sido usados para hospedar códigos maliciosos, devem retornar à categoria original depois de “descontaminados”;	
13.	**Características específicas do Item 55 - Appliance de Firewall/Filtro de Conteúdo - Regionais Tipo 1**	-
13.1.	Além das interfaces utilizadas para o link MPLS e para o link internet deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T, que serão utilizadas na rede interna da CONTRATANTE.	
13.2.	O throughtput de SSL inspection ou NFGFW ou Application Control, deve ser maior do que 70 Mbps (setenta megabits por segundo).	
13.3.	O throughtput de VPN, deve ser maior do que 70 Mbps (setenta megabits por segundo).	
13.4.	O throughtput de IPS, deve ser maior do que 70 Mbps (setenta megabits por segundo).	
13.5.	Deverá suportar no mínimo 50.000 (cinquenta mil) sessões de firewall simultâneas.	
14.	**Características específicas do item 56 - Appliance de Firewall/Filtro de Conteúdo - Regionais Tipo 2**	-
14.1.	Além das interfaces utilizadas para o link MPLS e para o link internet deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T, que serão utilizadas na rede interna da CONTRATANTE.	
14.2.	O throughtput de SSL inspection ou NFGFW ou Application Control, deve ser maior do que 90 Mbps (noventa megabits por segundo).	

14.3.	O throughtput de VPN, deve ser maior do que 90 Mbps (noventa megabits por segundo).	
14.4.	O throughtput de IPS, deve ser maior do que 90 Mbps (noventa megabits por segundo).	
14.5.	Deverá suportar no mínimo 60.000 (sessenta mil) sessões de firewall simultâneas.	
15.	**Características específicas do item 57 - Appliance de Firewall/Filtro de Conteúdo - Regionais Tipo 3**	-
15.1.	Além das interfaces utilizadas para o link MPLS e para o link internet deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T), que serão utilizadas na rede interna da CONTRATANTE.	
15.2.	O throughtput de SSL inspection ou NFGFW ou Application Control, deve ser maior do que 150 Mbps (cento e cinquenta megabits por segundo).	
15.3.	O throughtput de VPN, deve ser maior do que 150 Mbps (cento e cinquenta megabits por segundo).	
15.4.	O throughtput de IPS, deve ser maior do que 150 Mbps (cento e cinquenta megabits por segundo).	
15.5.	Deverá suportar no mínimo 80.000 (oitenta mil) sessões de firewall simultâneas.	
16.	**Características específicas do item 58 - Appliance de Firewall/Filtro de Conteúdo - Sede**	-
16.1.	As características abaixo se referem a 1 (uma) unidade do appliance.	-
16.2.	Além das interfaces utilizadas para gerência e para funcionamento do cluster deve possuir pelo menos 8 (oito) interfaces GigabitEthernet (10/100/1000Base-T e 4 (quatro) interfaces 10GigabitEthernet 10Gbase-SR, que serão utilizadas na rede interna da CONTRATANTE.	
16.3.	Deve ter no mínimo 2 (duas) fontes de alimentação;	
16.4.	Deve suportar a configuração em alta disponibilidade ativo/passivo e ativo/ativo e em caso de falha em um dos nós, o remanescente deverá assumir o controle automaticamente, mantendo as sessões correntes ativas;	
16.5.	O throughtput de SSL inspection ou NFGFW ou Application Control, deve ser maior do que 5.8 Gbps (seis gigabits por segundo).	
16.6.	O throughtput de VPN, deve ser maior do que 6 Gbps (seis gigabits por segundo).	
16.7.	O throughtput de IPS, deve ser maior do que 6 Gbps (seis gigabits por segundo).	
16.8.	Deverá suportar no mínimo 2.000.000 (dois milhões) de sessões de firewall simultâneas.	
16.9.	**Prevenção de ameaças**	-
16.9.1.	• Deve-se sincronizar as assinaturas de IPS quando implementado em alta disponibilidade ativo/ativo e ativo/passivo.	
16.10.	**Identificação de usuários**	-
16.10.1.	• Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (portal captivo);	
16.10.2.	• Deve implementar funcionalidade que possibilite analisar as informações de accounting do Microsoft NPS para permitir a identificação de usuários, como RSSO, Radius Accounting ou similar;	
16.10.3.	• Deve suportar a identificação de usuários via certificados	

	digitais ICP-Brasil para conexões a serviços via SSL VPN.	
16.11.	**VPN**	-
16.11.1.	• Suportar VPN client-to-site;	
16.11.2.	• Suportar IPSec VPN, com suporte a AES e autenticação via certificado IKE PKI;	
16.11.3.	• Suportar SSL VPN com as seguintes funcionalidades:	-
16.11.4.	◦ Que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;	
16.11.5.	◦ Que as funcionalidades de VPN SSL sejam atendidas sem o uso de cliente;	
16.11.6.	◦ Atribuição de endereço IP nos clientes remotos de VPN;	
16.11.7.	◦ Atribuição de DNS nos clientes remotos de VPN;	
16.11.8.	◦ Criar políticas de controle de aplicações, IPS, para trafego dos clientes remotos conectados na VPN SSL;	
16.11.9.	◦ Suportar autenticação via AD/LDAP, Secure id, certificado padrão ICP-Brasil e base de usuários local;	
16.11.10.	◦ Permitir estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;	
16.11.11.	◦ Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos tuneis SSL;	
16.11.12.	◦ O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows Vista Windows 7, Windows 8 e Mac Osx;	
16.11.13.	◦ A solução de segurança entregue deverá suportar e estar licenciada para pelo menos 2.000 (duas mil) conexões remotas simultaneas VPN SSL.	
16.12.	**Filtro de URLs**	-
16.12.1.	• Deve permitir os segmentos de rede funcionem de maneira diferente, com pelo menos as seguintes possibilidades: proxy explicito, proxy transparente, portal captivo.	
17.	**Item 59 - Solução de Gerência dos e Appliances de Firewall/Filtro de Conteúdo**	-
17.1.	Deve centralizar a administração de regras, políticas e geração de relatórios dos appliances de firewall/filtro de conteúdo, usando uma única interface de gerenciamento.	
17.2.	Deve ser disponibilizado em hardware próprio ou em servidor x86 com a capacidade adequada. Será permitida a utilização de solução de virtualização.	
17.3.	Pode ser disponibilizada no ambiente da CONTRATADA, com acesso pela rede MPLS.	
17.4.	**Deve permitir/possuir**	-
17.4.1.	• Acesso via cliente para Windows ou WEB (HTTPS);	
17.4.2.	• Autenticações integrada ao Microsoft Active Directory ou servidor Radius;	
17.4.3.	• Permitir a criação de grupos de dispositivos com a possibilidade de aplicar a mesma política em vários dispositivos de forma simultânea;	
17.4.4.	• Inspeção de logs com a possibilidade de exportar tais registros em formato CSV;	

17.4.5.	• Armazenamento de logs com capacidade de acesso instantâneo e capacidade de rotacionar tais registros;	
17.4.6.	• Busca de objetos como: regras, hosts, redes, aplicações;	
17.4.7.	• Definições de perfis de acesso a console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;	
17.4.8.	• Localização de em quais regras um endereço IP, IP Range, rede ou objetos estão sendo utilizados;	
17.4.9.	• Contador ou gráfico de matchs das regras;	
17.4.10.	• Contador ou gráfico de volume trafegado por cada regra;	
17.4.11.	• Backup das configurações com versionamento e aplicação de rollback para uma versão anterior;	
17.4.12.	• A visualização e comparação das configurações atuais de um appliance com configurações anteriores;	
17.4.13.	• A atualização de sistema operacional dos appliances bem como o rollback em caso de falha;	
17.4.14.	• A integração com outras soluções de SIEM de mercado (third-party SIEM vendors);	
17.4.15.	• Relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;	
17.4.16.	• Relatórios de utilização dos recursos por aplicações, URL e ameaças;	
17.4.17.	• Visualização sumarizada de todas as aplicações, ameaças e URLs que trafegaram pelos appliances;	
17.4.18.	• Cliente NTP, contemplando suporte à autenticação entre os peers;	
17.4.19.	• Agente SNMP nas versões 2c e 3, com suporte a MIB-II, possibilitando acesso de leitura com restrição dos endereços que podem efetuar consultas SNMP;	
17.5.	**Exibição das seguintes informações, de forma histórica:**	-
17.5.1.	• Situação dos appliances individuais e do cluster;	
17.5.2.	• Principais aplicações;	
17.5.3.	• Principais aplicações por risco;	
17.5.4.	• Administradores autenticados na gerencia da plataforma de segurança;	
17.5.5.	• Número de sessões simultâneas;	
17.5.6.	• Status das interfaces;	
17.5.7.	• Utilização das interfaces;	
17.5.8.	• Erros das interfaces;	
17.5.9.	• Uso de CPU;	
17.5.10.	• Memória RAM;	
17.6.	**Deve permitir visualizar as seguintes tabelas de informação (via dashboard ou linha de comando) para cada appliance e cluster**	-
17.6.1.	• MAC;	
17.6.2.	• ARP;	

17.6.3.	• De roteamento unicast, informando como a rota foi aprendida bem como qual é o próximo salto;	
17.6.4.	• De roteamento multicast, informando a origem e o status de cada grupo bem como a quantidade de pacotes encaminhados;	
17.6.5.	• O status de um dado link de dados (para a funcionalidade de balanceamento de ISP).	
17.7.	**Registro de informações de filtro de URLs**	-
17.7.1.	• Deverá manter os registros de conexão para o envio e recebimento de pacotes de dados com pelo menos os seguintes dados: data e hora de início e término, sua duração, usuário (quando houver identificação), o endereço IP de origem, URL de destino da requisição, categoria do site, tamanho do objeto solicitado (em bytes) e ação tomada pela solução (bloqueado, permitido);	
17.7.2.	• Deverá ser capaz de reter dados e logs nos modos on-line e off-line, em que:	
17.7.3.	• No modo on-line, os dados deverão ser mantidos disponíveis para consulta imediata por um período mínimo de 90 (noventa) dias;	
17.7.4.	• No modo off-line, os dados deverão ser arquivados na solução de backup da CONTRATANTE, sem acesso direto pela solução de gerência, e que precisam ser restaurados e reativados para consulta, disponíveis para consulta imediata por um período mínimo de 1 (um) ano;	
17.8.	**Geração de, no mínimo, os seguintes relatórios:**	-
17.8.1.	• Resumo gráfico de aplicações utilizadas;	
17.8.2.	• Principais aplicações por utilização de largura de banda de entrada e saída;	
17.8.3.	• Principais aplicações por taxa de transferência de bytes;	
17.8.4.	• Principais hosts por número de ameaças identificadas;	
17.8.5.	• Atividades de um usuário especifico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças, de rede vinculadas a este tráfego.	
17.8.6.	• Relatórios de filtro de URLs	-
17.8.7.	◦ Deve disponibilizar ferramenta para geração de relatórios, fornecendo informações gerenciais a partir dos logs gerados, permitindo a extração de informações detalhadas sobre usuários, sites e categorias acessadas, rede de origem, IP de origem, grupos de usuários, protocolos e tempo de navegação;	
17.8.8.	◦ Deve permitir a geração de relatório com a quantidade de acessos autorizados, bem como a quantidade de bytes trafegados, permitindo a visualização por usuário, grupo de usuário, IP de origem, aplicação e URL completa acessada;	
17.8.9.	◦ Deve possuir templates com pelos menos os seguintes relatórios:	
17.8.10.	• Lista de usuários com maior número de acessos;	
17.8.11.	• Lista de usuários que geraram maior volume trafegado;	
17.8.12.	• Lista de sites com maior número de acessos, incluindo detalhamento por usuário dos 2 (dois) sites com maior número de acessos;	
17.8.13.	• Lista de sites que geraram maior volume trafegado, incluindo detalhamento por usuário dos 2 (dois) sites com maior volume trafegado;	
17.8.14.	• Lista de categorias com maior número de acessos;	

17.8.15.	• Lista de categorias que geraram maior volume trafegado;	
17.8.16.	• Lista de sites bloqueados com maior número de tentativa de acessos;	
17.8.17.	• Lista de sites maliciosos com maior número de tentativa de acessos;	
17.8.18.	◦ Deve exportar relatórios para, no mínimo, os formatos PDF ou CSV;	
17.8.19.	◦ Deve possibilitar a automatização no envio a usuários pré-definidos ou publicação de relatórios;	
18.	**Item 60 - Solução de Netflow**	-
18.1.	Software e/ou ferramenta e/ou funcionalidade de gerenciamento capaz de receber e analisar tráfego dos roteadores e appliances de firewall/filtro de conteúdo utilizando Netflow, IPFIX ou similar.	
18.2.	A solução de netflow pode estar disponibilizada no ambiente da CONTRATADA, com acesso pela rede MPLS.	
18.3.	A solução deve ser dimensionada para suportar o tráfego de todos os links MPLS desta especificação técnica.	
18.4.	Deve ser capaz de agrupar os tráfegos em aplicações utilizando pelo menos os seguintes critérios, redes de origem/destino, protocolo da camada de transporte, lista de porta de origem/destino da camada de transporte. Deve ser possível visualizar gráficos de cada link separando o tráfego com base nas aplicações em cores diferentes. Deve ser possível atualizar o gráfico omitindo/mostrando cada uma das aplicações.	
18.5.	Deve ser capaz de agrupar os tráfegos em classes de QoS. Deve ser possível visualizar gráficos de cada link separando o tráfego com base nas classes de Qos com em cores diferentes. Deve ser possível atualizar o gráfico omitindo/mostrando cada uma das classes de QoS.	
18.6.	Deve permitir o agrupamento de interfaces de hosts diferentes, formando uma interface agregada para fins de detalhamento de tráfego.	
18.7.	Deve presentar em gráficos separados o tráfego de entrada e de saída de cada link.	
18.8.	Deve permitir a elaboração de relatórios dos fluxos de comunicação em que deve ser possível verificar IP de origem e destino, protocolo da camada de transporte, porta de origem e destino da camada de transporte.	
18.9.	Deve ter capacidade suficiente para o armazenamento de histórico de pelo menos 1 (um) dos seguintes requisitos: 1 (um) TB de dados ou 6 (seis) meses de informações.	
19.	**Características específicas dos itens 61 e 67 - Link Internet – Sede**	-
19.1.	**A taxa de transmissão deve variar conforme os valores abaixo descritos:**	-
19.1.1.	• 150 Mbps (cento e cinquenta megabits por segundo);	-
19.1.2.	• 200 Mbps (duzentos megabits por segundo);	-
19.1.3.	• 250 Mbps (duzentos e cinquenta megabits por segundo);	-
19.1.4.	• 300 Mbps (trezentos megabits por segundo);	-
19.1.5.	• 350 Mbps (trezentos e cinquenta por segundo).	-
19.2.	**Anti-DDOoS (Distributed Denial of Service)**	-
19.2.1.	• Solução integrada ao backbone da CONTRATADA que deve proteger 100% (cem por cento) do tráfego de entrada do link internet;	
19.2.2.	• A proteção suportará Flash Crowd, ou seja, quando ocorrer o crescimento do volume de tráfego legítimo acima do esperado (perfil de tráfego/baseline), a solução será capaz de diferenciar	

	o tráfego legítimo do malicioso, bloqueando apenas o tráfego proveniente de ataques;	
19.2.3.	• 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.	
19.2.4.	• A solução deve suportar a mitigação automática de ataques, incluindo, mas não se restringindo as seguintes técnicas:	
19.2.4.1.	◦ Whitelists;	
19.2.4.2.	◦ Blacklists;	
19.2.4.3.	◦ Limitação de taxa;	
19.2.4.4.	◦ Técnicas desafio-resposta;	
19.2.4.5.	◦ Descarte de pacotes mal formados;	
19.2.4.6.	◦ Técnicas de mitigação de ataques aos protocolos HTTP e DNS;	
19.2.4.7.	◦ Bloqueio por localização geográfica de endereços IP;	
19.2.4.8.	◦ Lista dinâmica de endereços bloqueados. Os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pela CONTRATADA devem ser removidos da referida lista.	
19.2.5.	• A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede para IPv4, incluindo, mas não se restringindo aos seguintes:	
19.2.5.1.	◦ Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;	
19.2.5.2.	◦ Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;	
19.2.5.3.	◦ Ataques que utilizam fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;	
19.2.5.4.	◦ Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);	
19.2.5.5.	◦ Quanto a ataques à camada de aplicação, para os protocolos HTTP e DNS, a solução deve manter uma lista dinâmica de endereços IP bloqueados.	
19.2.6.	• A CONTRATADA deve possuir, no mínimo, 2 (dois) centros de limpeza, cada um com capacidade de mitigação de ataques. Dos centros de limpeza, pelo menos um deverá estar em território nacional e pelo um deverá estar no exterior. Para a mitigação dos ataques de origem no território brasileiro não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro.	
19.2.7.	• A CONTRATADA deverá prover o serviço de mitigação sem limitação de duração, volume de tráfego, quantidade de pacotes, ataques nacionais ou internacionais, quantidade de eventos, requisições por segundo, intervalos entre os ataques.	
19.2.8.	• As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques.	
19.2.9.	• Em momentos de ataques DoS e DDoS, todo trafego limpo deve ser reencaminhado para a CONTRATANTE.	
19.2.10.	• Em nenhum caso será aceito bloqueio de ataques de DoS e DDoS por ACLs em roteadores de bordas.	
19.2.11.	• A mitigação de ataques deve iniciar no prazo máximo de 15 (quinze) minutos após sua detecção.	
19.3.	**Topologia e roteamento**	-

19.3.1.	• O serviço deverá ser fornecido com suporte a MP-BGP, ou seja, encaminhamento de tráfego IPv4 e IPv6.	
19.3.2.	• A rede de trânsito entre os roteadores internet e o cluster de appliances de firewall/filtro de conteúdo da sede utilizará endereçamento IPv4 e IPv6 pertencentes ao AS da CONTRATANTE.	
19.3.3.	• A CONTRATADA deverá divulgar o AS (16 bits) e os blocos de endereços IPv4 e IPv6 da CONTRATANTE que serão divulgados pelos CPEs. Deve permitir a divulgação de blocos IPv4 /22, /23 e /24 e blocos IPv6 /44 e /48.	
19.3.4.	• A CONTRATADA deverá disponibilizar o seguinte conjunto de endereços:	-
19.3.4.1.	◦ 1 (um) endereço IPv4 (/32) para a interface de Loopback do CPE;	-
19.3.4.2.	◦ 1 (um) endereço IPv6 (/128) para a interface de Loopback do CPE;	-
19.3.4.3.	◦ 1 (um) bloco IPv4 /30 (ou /31) para o Link ponto-a-ponto da interface WAN;	-
19.3.4.4.	◦ 1 (um) bloco IPv6 /64 ou /127 para o Link ponto-a-ponto da interface WAN.	-
19.3.5.	• A vizinhança iBGP (IPv4 e IPv6) entre os dois CPEs bem como a vizinhança eBGP (IPv4 e IPv6) entre cada CPE e o PE da CONTRATADA devem ser estabelecidas utilizando os seguintes requisitos:	
19.3.5.1.	◦ Interfaces de loopback;	
19.3.5.2.	◦ TTL-Security habilitado;	
19.3.5.3.	◦ Autenticação MD5;	
19.3.5.4.	◦ Fornecimento de tabela parcial (partial routing) e tabela completa (full routing) para IPv4. A CONTRATANTE poderá optar pela tabela parcial ou tabela completa conforme solicitação. A tabela parcial deve incluir seleção definida pela CONTRATADA que inclua os ASes nacionais e internacionais com maior interesse de tráfego.	
19.3.5.5.	◦ A tabela partial deve conter no mínimo os principais ASes dos seguintes serviços de CDN, nuvem e provedores de conteúdo: Akamai, Amazon, Facebook, IBM, Google, Microsoft, Oracle, Rackspace, SoftLayer, Youtube. Por principais ASes entende-se aqueles da Europa e América, não havendo necessidade de prever ASes da Africa, Ásia e Oceania.	
19.3.5.5.1.	◦ Caso a tabela de parcial da CONTRATADA não forneça os ASes solicitados pela CONTRATANTE, será permitido o fornecimento da tabela completa (full routing) IPv4 desde que seja possível limitar as rotas a serem inseridas na tabela de roteamento com base no tamanho do AS Path a ser definido pela CONTRATANTE.	
19.3.5.6.	◦ Fornecimento de tabela completa IPv6 (full routing).	
19.3.6.	• A CONTRATADA deverá disponibilizar à CONTRATANTE a possibilidade de “negação de tráfego” à CONTRATANTE através de uso de uma community BGP de “blackhole/sinkhole” (buraconegro/vertedouro) em anúncio BGP da CONTRATANTE.	
19.3.7.	• Deverão ser aceitos para o efeito de “blackhole”, em IPv4: prefixos com tamanhos /24 e /32.	
19.3.8.	• Deverão ser aceitos para o efeito de “blackhole”, em IPv6: prefixos com tamanhos /32, /48, /56, /64 e /128.	
20.	**Itens 62 e 68 - Roteador Internet - Sede**	-
20.1.	As características abaixo se referem a 1 (uma) unidade do roteador.	-
20.2.	Além da interface utilizada para o link Internet deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T, que serão utilizadas pela CONTRATANTE.	

20.3.	Deve ter no mínimo 2 (duas) fontes de alimentação.	
20.4.	Possuir capacidade de comutação agregada igual ou superior à 2,5 Gbps (dois vírgula cinco gigabits por segundo)	
20.5.	Possuir capacidade de encaminhamento igual ou superior a 4 Mpps (quatro milhões de pacotes por segundo).	
20.6.	Possuir capacidade de memória RAM no processador central de no mínimo 1 GB (um gigabyte).	
20.7.	Possuir capacidade para 1.000.000 (um milhão) de prefixos IPv4 (FIB).	
20.8.	Possuir capacidade para 250.000 (duzentos e cinquenta mil) prefixos IPv6 (FIB).	
20.9.	**Devem suportar os seguintes protocolos/funcionalidades:**	-
20.10.	• O serviço deve permitir a administração remota, protegida por autenticação usuário/senha e utilizando pelo menos os protocolos SSHv2 e HTTPS;	
20.11.	• Implementar RFC 3768 VRRP;	
20.12.	• OSPFv2 e OSPFv3 com suporte a autenticação de vizinhança utilizando protocolo MD5;	
20.13.	• Cliente NTP, contemplando suporte à autenticação entre os peers, conforme definido na RFC 1305. Deve possibilitar a especificação da interface de origem dos pacotes NTP;	
20.14.	• Agente SNMP nas versões 2c e 3, com suporte a MIB-II, possibilitando acesso de leitura com restrição dos endereços que podem efetuar consultas SNMP;	
20.15.	• Capacidade de geração e armazenamento de logs locais;	
20.16.	• Protocolo Syslog com a possibilidade de envio de timestamp baseado no relógio do roteador;	
20.17.	• Protocolo IP SLA ou similar, ou sejam deve ser capaz de responder a pacotes de simulação de tráfegos. Devem ser suportados, no mínimo, os protocolos ICMP, TCP e UDP. Os dados referentes aos tráfegos simulados devem ser disponibilizados via SNMP;	
20.18.	• Implementar ACLs com pelo menos os seguintes parâmetros;	-
20.18.1.	◦ Endereços IP de host ou rede, de pacotes Ipv4 e Ipv6 (tanto de origem quanto de destino);	
20.18.2.	◦ Tipos de pacote ICMP;	
20.18.3.	◦ Portas e faixas de portas dos protocolos TCP e UDP (tanto de origem quanto de destino);	
20.18.4.	◦ Deve permitir criar regras com base em hora do dia e com base nos dias da semana;	
20.19.	• Protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow, IPFIX ou similar, contemplando no mínimo as seguintes informações:	
20.19.1.	◦ IP de origem/destino;	
20.19.2.	◦ Parâmetro “protocol type” do cabeçalho IP;	
20.19.3.	◦ Porta TCP/UDP de origem/destino;	
20.19.4.	◦ Campo TOS ou DSCP do cabeçalho IP;	
20.19.5.	◦ Interface do equipamento em que o tráfego foi identificado;	
20.19.6.	◦ A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo padrão de mercado para este fim;	

20.20.	• BGP	-
20.20.1.	◦ Implementar RFC 4271 BGPv4.	
20.20.2.	◦ Implementar RFC 1997 Communities and Attributes.	
20.20.3.	◦ Implementar RFC 4360 BGP Extended Communities Attribute.	
20.20.4.	◦ Implementar RFC 2918 Route Refresh Capability.	
20.20.5.	◦ Implementar RFC 2385 BGP Session Protection via TCP MD5.	
20.20.6.	◦ Implementar Generalized TTL Security Mechanism (GTSM).	
20.20.7.	◦ Implementar RFC 4893 BGP Support for Four-octet AS Number Space.	
20.20.8.	◦ Implementar Outbound Route Filtering Capability for BGP-4.	
20.20.9.	◦ Implementar RFC 2858 Multiprotocol Extensions for BGP-4.	
20.20.10.	◦ Implementar RFC 4724 Graceful Restart Mechanism for BGP.	
20.20.11.	◦ Implementar definição de políticas de controle dos anúncios BGP.	
20.20.12.	◦ Implementar aplicação de expressões regulares para filtragem de anúncios	
21.	**Item 63 - Serviço de Mudança de Endereço**	-
21.1.	Qualquer unidade poderá ter sua localização alterada, dentro dos limites de cada município.	-
21.2.	A instalação física e lógica do canal de comunicação no novo endereço deverá ser realizada em até 60 (sessenta) dias corridos, a contar da emissão da ordem de serviço pela CONTRATANTE;	-
21.3.	Todas as ações de funcionários da CONTRATADA dentro das dependências das Unidades da CONTRATANTE deverão ser executadas na presença do responsável da CONTRATANTE ou representantes por ela estabelecidos.	-
21.4.	A CONTRATANTE informará à CONTRADA exata em que a mudança do circuito deve ser realizada com pelo menos 3 (três) dias úteis de antecedência.	-
21.5.	A mudança poderá ocorrer em dias não úteis sem que haja qualquer custo adicional para a CONTRATANTE.	-
22.	**Item 64 - Implantação solução - Lote 1**	-
22.1.	Deverão ser apropriados neste contratado todos os custos para a implantação de infraestrutura dos itens 1 a 62 como: lançamento de fibras, construção de dutos, mão de obra para instalar e configurar os equipamentos, dentre outros custos existentes apenas na fase de instalação.	-
22.2.	Não deverão ser apropriados neste item os custos referentes aos equipamentos utilizados exclusivamente no provimento do serviço e que serão discriminados nos itens 28, 55 a 60 e 62.	-
22.3.	Não deverão ser apropriados neste item os custos referentes aos repasses de conhecimento e que serão discriminados nos itens 65 e 66.	-
23.	**Item 65 - Repasse de Conhecimento - Solução Firewall/Filtro de Conteúdo**	-
23.1.	A prestação do serviço de transferência de conhecimento deverá observar o disposto no Anexo III - ESPECIFICAÇÃO DOS SERVIÇOS DE TRANSFERENCIA DE CONHECIMENTO.	-
23.2.	**Deve abordar pelo menos os seguintes tópicos:**	-
23.2.1.	• Conhecimento e usabilidade dos recursos (hardwares e softwares) envolvidos;	-

23.2.2.	• Compreensão geral da filosofia de funcionamento e de operação da solução adotada;	-
23.2.3.	• Criação de grupos de dispositivos para aplicação de configurações em lote;	-
23.2.4.	• Criação/configuração e aplicação de regras com controle de aplicação;	-
23.2.5.	• Criação/configuração e aplicação de regras com filtro de URL;	-
23.2.6.	• Criação/configuração e aplicação de regras com SSL Inspection;	-
23.2.7.	• Criação/configuração e aplicação de regras com NAT estático e dinâmico;	-
23.2.8.	• Serviços de prevenção de ameaças;	-
23.2.9.	• VPN site-to-site;	-
23.2.10.	• SSL VPN;	-
23.2.11.	• Verificação de logs;	-
23.2.12.	• Backup e restauração de configuração;	-
23.2.13.	• Geração de relatórios gerenciais.	-
24.	**Itens 66 e 70 - Repasse de Conhecimento - Roteador Internet - Sede**	-
24.1.	A prestação do serviço de transferência de conhecimento deverá observar o disposto no Anexo III - ESPECIFICAÇÃO DOS SERVIÇOS DE TRANSFERENCIA DE CONHECIMENTO.	-
24.2.	**Deve abordar pelo menos os seguintes tópicos:**	-
24.2.1.	• O Protocolo BGP e seus Pacotes;	-
24.2.2.	• MP-BGP;	-
24.2.3.	• Vizinhança BGP (IPv4/IPV6, autenticação, TTL e uso de loopback);	-
24.2.4.	• iBGP e eBGP;	-
24.2.5.	• Atributos do BGP (Origin, AS Path, Next Hop, MED, Local Preference, Weight, Aggregator e Community);	-
24.2.6.	• Algoritmo para escolha do melhor caminho utilizado pelo BGP;	-
24.2.7.	• Filtros de entrada e saída;	-
24.2.8.	• Expressões regulares;	-
24.2.9.	• Boas práticas de BGP para sistemas autônomos;	-
24.2.10.	• Conectando a um IXP.	-
25.	**Item 69 - Implantação solução - Lote 2**	-
25.1.	Deverão ser apropriados neste contratado todos os custos para a implantação de infraestrutura do item 67 como: lançamento de fibras, construção de dutos, mão de obra para instalar e configurar os equipamentos, dentre outros custos existentes apenas na fase de instalação.	-
25.2.	Não deverá ser apropriado neste item o custo referente ao equipamento utilizado no provimento do serviço e que será discriminado no item 68.	-
25.3.	Não deverá ser apropriado neste item o custo referente ao repasse de conhecimento e que será discriminado no item 70.	-

ANEXO II DO TERMO DE REFERENCIA

definição DOS NÍVEIS mínimos DE SERVIÇO

1. Todos os equipamentos devem ser dimensionados para suportar os requisitos informados na especificação técnica. Os dispositivos que apresentem alta utilização de recursos devem ser substituídos por outros de maior capacidade. Por alta utilização de recursos entende-se qualquer uma das situações descritas abaixo:
    1. Quando a soma dos períodos (dentro de um mês específico) em que o equipamento permaneceu com a CPU (ou média da utilização das CPUs) acima de 70% (setenta porcento) for maior do que 8 (oito) horas;
    1. Quando a soma dos períodos (dentro de um mês específico) em que o equipamento permaneceu com a utilização da memória RAM acima de 80% (sessenta porcento) for maior do que 16 (dezesseis) horas;
2. O prazo para substituir os equipamentos será de 60 (sessenta) dias, sem prejuízos das eventuais glosas e multas decorrentes dos esgotamentos dos recursos computacionais;
3. Não será necessário efetuar a substituição dos equipamentos nas situações em que a CONTRATADA utilizar tráfego superior aos maiores valores definidos nas especificações dos itens;
4. Nem o perfil de tráfego da CGU e nem a utilização de recursos que não fazem parte da especificação poderão ser utilizados como argumento para a alta utilização dos recursos; Não será permitido que recursos técnicos sejam desabilitados para reduzir o consumo computacional dos dispositivos;
5. Os links MPLS deverão possuir latência de, no máximo, 150 ms (cinquenta milissegundos) e os links Internet deverão possuir latência de, no máximo, 65 ms (sessenta e cinco milisegundos).
    5. A latência será considerada como o tempo em que um pacote IP leva para ir de um ponto a outro da rede e retornar à origem.
6. Os links MPLS e Internet deverão possuir perda de pacotes de no máximo 1% (um por cento).
    6. Para o cálculo deste parâmetro serão considerados erros de interface, pacotes corrompidos pelo Link, erros de CRC, bem como descartes injustificados por parte do roteador;
7. As amostras de latência e perda de pacotes deverão ser coletadas a cada 05 (cinco) minutos;
8. Para os links Internet, as medições de latência e perda de pacotes devem ser feitas entre o Roteador Internet ou Appliance de Firewall/Filtro de Conteúdo e o primeiro roteador da CONTATADA na Internet;
9. Para os links MPLS das regionais, as medições de latência e perda de pacotes devem ser feitas entre um Roteador da Sede e o Appliance de Firewall/Filtro de Conteúdo da referida unidade regional;
10. Para os links MPLS da Sede, as medições de latência e perda de pacotes devem ser feitas entre cada Roteador da Sede e o centro de gerência da CONTRADA;
11. A cada medição que apresentar aferições de latência e perda de pacotes superiores aos valores especificados deverá ser considerada como períodos de indisponibilidade, obedecidas as seguintes condições:
    11. Cada medição deve ser considerada como 5 (cinco) minutos de indisponibilidade;
    11. Caso ocorram violações simultâneas de latência e perda de pacotes, apenas uma indisponibilidade deve ser calculada;
    11. Caso ocorram violações de latência e perda de pacotes no link MPLS da Sede utilizado como referência para aferir os parâmetros em relação aos links regionais, não é necessário calcular indisponibilidades por esses motivos para os links MPS das regionais;
    11. Não serão consideradas medições de pacotes atrasados/descartados em momentos de esgotamento da capacidade do link, situações definidas quando a utilização de entrada ou de saída for superior a 80% (oitenta por cento) da utilização da taxa contratada;
12. A indisponibilidade dos Appliances de Firewall/Filtro de Conteúdo das unidades regionais implicará automaticamente na indisponibilidade dos serviços dos links MPLS e Internet dessas unidades;
13. A indisponibilidade do cluster de Appliances de Firewall/Filtro de Conteúdo da Sede ou do Roteador da Sede implicará automaticamente na indisponibilidade do serviço de link Internet desta unidade (apenas do lote 1);
14. A disponibilidade do serviço corresponde ao percentual de tempo, durante o período de 1 (um) mês, em que o mesmo esteve em condições normais de funcionamento. Além das condições citadas acima, serão considerados como períodos de indisponibilidade o tempo em que o serviço estiver total ou parcialmente indisponível;
15. Os serviços deverão possuir disponibilidade de, no mínimo, 99,44% (noventa e nove vírgula quarenta e quatro por cento);
16. Não serão consideradas indisponibilidades as seguintes situações:
17. Paradas programadas pela CONTRATADA e aprovadas pela CGU. Neste caso, a autorização deve ser solicitada pela CONTRATADA com, pelo menos, 5 (cinco) dias úteis de antecedência;
18. Paradas ocasionadas com erros de configuração dos equipamentos causados pela CGU, sem responsabilidade da CONTRATADA;
19. O Índice de Disponibilidade Mensal da solução será calculado através da seguinte fórmula:

$$\textbf{IDM(\%)} = ((\textbf{Tm} - \textbf{Ti}) / \textbf{Tm}) * 100\%$$

Em que:

IDM: é o Índice de Disponibilidade Mensal do serviço, com duas casas decimais;

Tm: é o tempo total mensal de operação, em minutos, no mês de medição. Para o cálculo do índice de disponibilidade, o "tempo total mensal" será calculado a partir do total de dias da prestação do serviço vezes 1440 (mil quatrocentos e quarenta) minutos;

Ti: é o somatório dos períodos considerados como de indisponibilidade (excetuando-se as paradas internas sob responsabilidade da CGU), em minutos, no mês de medição.

20. Os serviços contratados serão considerados indisponíveis a partir do momento em que eventuais problemas forem detectados até o seu retorno às condições plenas de funcionamento;
21. A apuração e/ou contabilização das grandezas acima definidas, para efeito de aferição de resultados, dar-se-á mensalmente;
22. O período de indisponibilidade (Ti) será glosado proporcionalmente na fatura mensal em relação ao tempo total mensal de operação (Tm), caso o **IDM** seja menor que 99,44%, conforme o seguinte cálculo:

$$\textbf{G} = (99{,}4\% - \textbf{IDM(\%)}) * \textbf{VMF}$$

Em que:

G: Valor Total da Glosa.

IDM: Índice de Disponibilidade Mensal;

VMF: Valor mensal da fatura;

ANEXO III DO TERMO DE REFERÊNCIA

ESPECIFICAÇÃO DOS SERVIÇOS DE TRANSFERENCIA DE CONHECIMENTO

1. Os serviços de transferência será composto por módulos Operacionais e Administrativos que devem consistir na oferta de cursos presenciais em Brasília/DF com abordagem prática voltada a todos os requisitos funcionais da solução contratada;

2. A CONTRATADA deverá apresentar uma proposta para um Plano de Repasse de Conhecimentos com realização em Brasília-DF. O plano de repasse a ser fornecida pela CONTRATADA deverá conter, no mínimo, os seguintes itens:

2.1. Cronograma;

2.2. Conteúdo programático;

2.3. Carga horária; e

2.4. Previsão de local, data e hora da realização dos eventos.

3. Os serviços se realização de forma presencial em Brasília-DF;

4. As turmas serão compostas por 06 (seis) alunos oficiais, mais 2 (dois) alunos na condição de ouvintes;

5. Os locais de realização das aulas serão providos pela CONTRATADA;

6. O material didático, meios audiovisuais e estrutura de TI necessária para realização do curso serão providos pela CONTRATADA;

6.1. Para atendimento ao item 65, o material didático deverá ser material oficial do FABRICANTE da solução.

7. Os cursos serão ministrados em língua portuguesa;

8. Deverá utilizar a infraestrutura física de responsabilidade da CONTRATADA e deverá ser do tipo hands-on;

8.1. Deve empregar laboratório (que pode ser físico ou virtual) com pelo menos 1 (um) POD por aluno. O laboratório deve utilizar equipamentos do mesmo fabricante, com as mesmas funcionalidades e interface/sintaxe dos utilizados para atender a solução de firewall/filtro de conteúdo.

9. Deverá ser entregue comprovação da capacitação dos instrutores no prazo de 5 (cinco) dias úteis a contar da data da reunião inicial;

9.1. Para atendimento ao item 65, a comprovação da capacitação dos instrutores deverá ser fornecida pelo FABRICANTE.

10. Para atendimento ao item 65, o processo transferência de conhecimentos deverá ser oficial do FABRICANTE da solução, com emissão de certificado de participação, impresso em papel timbrado;

11. Para os itens 66 e 70, o processo de transferência de conhecimentos deverá ser ministrado por instrutor com conhecimento sobre a solução, de forma a garantir que todos os requisitos necessários para operação, gerência e manutenção da solução sejam ministrados com a carga horária adequada;

12. Ao final da transferência de conhecimentos, deverá ser realizada uma avaliação do curso;

12.1. Ao término do processo de transferência de conhecimentos, a contratada deverá realizar uma avaliação de satisfação em relação ao curso, como conteúdo, instalações, material didático e de aplicação à prática profissional, bem como do(s) instrutor(es). Caso o curso seja considerado insatisfatório, a contratada deverá realizar um novo processo de transferência de conhecimentos, com a finalidade de atender as demandas não supridas inicialmente. Um relatório contendo a avaliação de satisfação dos alunos deverá ser enviado a CGU.

13. Deverá ser fornecida documentação técnica completa e atualizada, contendo manuais, guias de instalação e configuração, melhores práticas e outros pertinentes, todos originais e uma cópia digitalizada em meio eletrônico desta mesma documentação;

14. A CGU não assumirá os custos de licenças e/ou softwares extras, diárias e transporte dos instrutores, assim como outros custos relativos a esta capacitação. Todos os custos devem ser previstos pela CONTRATADA/FABRICANTE da solução na elaboração de suas propostas;

14.1. Não serão de responsabilidade da CONTRATADA os custos de transporte e diárias dos participantes da CONTRATANTE.

ANEXO IV DO TERMO DE REFERÊNCIA

MODELOS DOS DOCUMENTOS DE HABILITAÇÃO

ATESTADO DE CAPACIDADE TÉCNICA (SERVIÇO MPLS)

O(a) Sr(a) [*nome do(a) responsável*], CPF [*número do CPF do responsável*], cargo [*cargo que ocupa*], na [*Nome (Razão Social) da Empresa Contratante*], CNPJ [*número do CNPJ da Contratante*], endereço [*endereço completo*], atesta, sob as penas da Lei, que a empresa [*Nome (Razão Social) da Empresa Contratada*], CNPJ [*número do CNPJ da Contratada*], com sede à [*endereço completo da Contratada*], forneceu (fornece) serviço rede WAN MPLS (Multiprotocol Label Switching) que interligou unidades em [*número de unidades da federação*] diferentes estados brasileiros com Links iguais ou superiores a [*taxa de transmissão*] Mbps, tendo prestado os referidos serviços de **forma satisfatória**, no período de [*dd/mm/aaaa*] a [*dd/mm/aaaa*]**.**

_____

[*Local e data da emissão do Atestado*]

_____

[*Assinatura do responsável pela emissão do Atestado, com nome, cargo, telefone e e-mail institucional para contato.*]

ATESTADO DE CAPACIDADE TÉCNICA (LINK INTERNET)

O(a) Sr(a) [*nome do(a) responsável*], CPF [*número do CPF do responsável*], cargo [*cargo que ocupa*], na [*Nome (Razão Social) da Empresa Contratante*], CNPJ [*número do CNPJ da Contratante*], endereço [*endereço completo*], atesta, sob as penas da Lei, que a empresa [*Nome (Razão Social) da Empresa Contratada*], CNPJ [*número do CNPJ da Contratada*], com sede à [*endereço completo da Contratada*], forneceu (fornece) serviço Link Internet com Link igual ou superior a [*taxa de transmissão*] Mbps, tendo prestado os referidos serviços de **forma satisfatória**, no período de [*dd/mm/aaaa*] a [*dd/mm/aaaa*]**.**

_____

[*Local e data da emissão do Atestado*]

_____

[*Assinatura do responsável pela emissão do Atestado, com nome, cargo, telefone e e-mail institucional para contato.*]

ANEXO V - MINUTA DO TERMO DE CONFIDENCIALIDADE

TERMO DE CONFIDENCIALIDADE

CONTRATO Nº _____ / _____

A **<PESSOA JURÍDICA OU FÍSICA CONTRATADA>** doravante referida simplesmente como **CONTRATADA**, inscrita no CNPJ/MF sob o número <NÚMERO DO CNPJ>, com endereço <ENDEREÇO>, neste ato representada pelo <VÍNCULO DO SIGNÁRIO COM A CONTRATADA>, **<NOME DO SIGNATÁRIO>**, nos termos do <CONTRATO OU TERMO ADITIVO EM QUE FOI PACTUADO O SIGILO>, compromete-se a observar o presente TERMO DE CONFIDENCIALIDADE, firmado perante a **UNIÃO**, por meio do **MINISTÉRIO DA TRANSPARÊNCIA, FISCALIZAÇÃO E CONTROLADORIA GERAL DA UNIÃO,** doravante referido simplesmente como **CGU**, em conformidade com as cláusulas que seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste TERMO DE CONFIDENCIALIDADE é a necessária e adequada proteção às informações controladas de propriedade exclusiva da CGU fornecidas à CONTRATADA para que possa desenvolver as atividades contempladas especificamente no Contrato nº _____/201X.

Subcláusula Primeira - A CONTRATADA reconhece que, em razão da prestação de serviços à CGU, tem acesso a informações que pertencem à CGU, que devem ser tratadas como controladas.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

O termo "informações controladas de propriedade exclusiva da CGU" abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outras a que, diretamente ou através de seus empregados, prepostos ou prestadores de serviço, venha a CONTRATADA ter acesso durante ou em razão da execução do contrato celebrado.

Subcláusula Primeira - Em caso de dúvida acerca da natureza confidencial de determinada informação, a CONTRATADA deverá mantê-la sob sigilo até que seja autorizada expressamente pelo representante legal da CGU, referido no Contrato, a tratá-la diferentemente. Em hipótese alguma, a ausência de manifestação expressa da CGU poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA - DAS OBRIGAÇÕES

A CONTRATADA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa da CGU, das informações controladas reveladas.

Subcláusula Primeira – As informações de caráter técnico observadas ou informadas durante a execução do contrato que impactem especificamente os produtos ou serviços fornecidos e prestados pela CONTRATADA poderão ser utilizadas por essa para a melhoria de seus produtos, reparos ou mesmo compartilhados com outros clientes sem a necessidade de autorização prévia da CGU. Em nenhum momento o nome da CGU ou outra fonte poderá ser vinculada ou distribuída conjuntamente com a informação dos produtos da CONTRATADA.

Subcláusula Segunda - A CONTRATADA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços à CGU, as informações controladas reveladas.

Subcláusula Terceira - A CONTRATADA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços aa CGU, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações controladas reveladas.

Subcláusula Quarta - A CONTRATADA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

Subcláusula Quinta - A CONTRATADA obriga-se a informar imediatamente à CGU qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

CLÁUSULA QUARTA - DO DESCUMPRIMENTO

A quebra do sigilo das informações controladas reveladas, devidamente comprovada, sem autorização expressa da CGU, possibilitará a imediata rescisão de qualquer contrato firmado entre a CGU e a CONTRATADA sem qualquer ônus para a CGU. Nesse caso, a CONTRATADA estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CGU, inclusive os de ordem moral, bem como as responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

CLÁUSULA QUINTA - DO RETORNO DAS INFORMAÇÕES

A CONTRATADA devolverá imediatamente à CGU, ao término do Contrato, todo e qualquer material de propriedade desta, inclusive registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada confidencial, nos termos do presente TERMO DE CONFIDENCIALIDADE, a que teve acesso em decorrência do vínculo contratual com a CGU.

CLÁUSULA SEXTA - DA VIGÊNCIA

O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor a partir de sua assinatura e enquanto perdurar a natureza sigilosa ou restrita da informação, inclusive após a cessação da razão que ensejou o acesso à informação.

CLÁUSULA SÉTIMA - DAS DISPOSIÇÕES FINAIS

Os casos omissos neste TERMO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pela CGU.

Por estarem de acordo, a CONTRATADA, por meio de seu representante, firma o presente TERMO DE CONFIDENCIALIDADE, lavrando em duas vias de igual teor e forma.

Brasília, DF, _____ de _____ de _____.

<REPRESENTANTE DA CONTRATADA>

<VÍNCULO DO REPRESENTANTE COM A CONTRATADA> RG: CPF:
DE ACORDO: (integrantes da equipe técnica da CONTRATADA) _____ _____ Nome: Nome: RG: RG:

ANEXO VI – MINUTA DO TERMO DE RESPONSABILIDADE E SIGILO

TERMO DE RESPONSABILIDADE E SIGILO

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste TERMO DE RESPONSABILIDADE E SIGILO é a necessária e adequada proteção às informações controladas de propriedade exclusiva da CGU fornecidas à LICITANTE para que possa realizar a vistoria técnica prevista neste TR.

Subcláusula Primeira - A LICITANTE reconhece que, em razão da participação do processo licitatório, tem acesso a informações que pertencem à CGU, que devem ser tratadas como controladas.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

O termo "informações controladas de propriedade exclusiva da CGU" abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outras a que, diretamente ou através de seus empregados, prepostos ou prestadores de serviço, venha a LICITANTE ter acesso durante ou em razão da execução do processo licitatório.

Subcláusula Primeira - Em caso de dúvida acerca da natureza confidencial de determinada informação, a LICITANTE deverá mantê-la sob sigilo. Em hipótese alguma, a ausência de manifestação expressa da CGU poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA - DAS OBRIGAÇÕES

A LICITANTE compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa da CGU, das informações controladas reveladas.

Subcláusula Primeira – Em nenhum momento o nome da CGU ou outra fonte poderá ser vinculada ou distribuída conjuntamente com a informação dos produtos da LICITANTE.

Subcláusula Segunda - A LICITANTE compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no Termo de Referência e em seus anexos, as informações controladas reveladas.

Subcláusula Terceira - A LICITANTE deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas ao processo licitatório, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações controladas reveladas.

Subcláusula Quarta - A LICITANTE possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

Subcláusula Quinta - A LICITANTE obriga-se a informar imediatamente à CGU qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

CLÁUSULA QUARTA - DO DESCUMPRIMENTO

A quebra do sigilo das informações controladas reveladas, devidamente comprovada, sem autorização expressa da CGU, possibilitará a imediata exclusão da LICITANTE do certame. Nesse caso, a LICITANTE estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CGU, inclusive os de ordem moral, bem como as responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

CLÁUSULA QUINTA - DA VIGÊNCIA

O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor a partir de sua assinatura e enquanto perdurar a natureza sigilosa ou restrita da informação, inclusive após a cessação da razão que ensejou o acesso à informação.

CLÁUSULA SEXTA - DAS DISPOSIÇÕES FINAIS

Os casos omissos neste TERMO DE RESPONSABILIDADE E SIGILO, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pela CGU.

Por estarem de acordo, a LICITANTE, por meio de seu representante, firma o presente TERMO DE RESPONSABILIDADE E SIGILO, lavrando em duas vias de igual teor e forma.

Brasília, DF, _____ de _____ de 2017.

<REPRESENTANTE DA LICITANTE>

<VÍNCULO DO REPRESENTANTE COM A LICITANTE>

RG:

CPF:

DE ACORDO:

(Integrantes da equipe técnica da LICITANTE)

_____	_____
Nome:	Nome:
RG:	RG:

ANEXO VII DO TERMO DE REFERENCIA

endereÇOS da Ministério da Transparência, Fiscalização e Controladoria-Geral da União

Unidade Sede

End.: Setor de Autarquias Sul, Quadra 01, Bloco A, Ed. Darcy Ribeiro, Almoxarifado

Brasília/DF - CEP: 70.070-905

Tel.: (61) 2020-7000

Unidade Regional - Acre

End.: Via Chico Mendes, nº 2896 Bairro Triângulo Novo

Rio Branco/AC - CEP: 69.906-302

Tel.: (68) 3223-2901 Ramal: 2501/ 2500

Unidade Regional - Alagoas

End.: Avenida Comendador Gustavo Paiva, nº 2.789, Salas 409 a 414, Ed. Norcon Empresarial, Mangabeiras

Maceió/AL - CEP: 57.031-000

Tel.: (82) 4009-6350

Unidade Regional - Amapá

End.: Av. Duque de Caxias, 116, Santa Rita, Macapá/AP

Tel.: (96) 2101-9230 ramais: 9231 / 9232 / 9233 / 9234 / 9235 / 9236

Unidade Regional - Amazonas

End.: Av. Japurá, nº 329 - Centro

Manaus/AM - CEP: 69.025-020

Tel.: (92) 3233-6628 / 6252 / 2129-0163

Unidade Regional - Bahia

End.: Avenida Frederico Pontes, s/nº, Ed. Min. da Fazenda, 2º andar, Sala 200 - Comércio

Salvador/BA - CEP: 40.015-902

Tel.: (71) 3254-5211 / (71) 3254-5212

Unidade Regional - Ceará

End.: Rua Barão de Aracati, nº 909, 8º andar - Bairro Meireles

Fortaleza/CE - CEP: 60.115-081

Tel.: (85) 3878-3800

Fax: (85) 3878-3824 / 3878-3822

Unidade Regional - Espírito Santo

End.: Rua Pietrangelo de Biase, nº 56, 4º andar, Sala 404 - Centro

Vitória/ES - CEP: 29.010-190

Tel.: (27) 3211-5262

Unidade Regional - Goiás

End.: Rua 02, n° 49, Ed. Walter Bittar - Centro

Goiânia/GO - CEP: 74.013-020

Tel.: (62) 3901-4360 / (62) 3901-4400

Unidade Regional - Maranhão

End.: Avenida dos Holandeses, lote 08, Quadra 35, 1º, 2º e 3º Pavimentos - Bairro do Calhau

São Luís/MA - CEP: 65.071-380

Tel.: (98) 3194-2000/ (98) 3268-4088

Unidade Regional - Minas Gerais

End.: Rua Timbiras, nº 1.778, Lourdes

Belo Horizonte/MG - CEP: 30.140-061

Tel.: (31) 3239-7200

Unidade Regional - Mato Grosso do Sul

End.: Avenida Joaquim Murtinho, nº 65 - Centro

Campo Grande/MS - CEP: 79.002-100

Tel.: (67) 3384-7777, Ramal 3303-4450

Unidade Regional - Mato Grosso

End.: Avenida Vereador Juliano Costa Marques, nº 99, Prédio do Ministério da Fazenda, 2º andar – Jardim Aclimação

Cuiabá/MT - CEP: 78.050-907

Tel.: (65) 2193-0437 / (65) 3615-2243

Unidade Regional - Pará

End.: Rua dos Mundurucus, nº 3100 – Ed. Metropolitan, 27º andar - Cremação

Belém/PA - CEP: 66.033-040

Tel.: (91) 3222-9446/ (91) 3205-8394

Unidade Regional - Paraíba

End.: Avenida Presidente Epitácio Pessoa, nº 3883, Bairro Miramar. Ed. Sede da CGU.

João Pessoa/PB - CEP: 58.032-000

Tel.: (83) 2108-3047/ (83) 2108-3046

Fax: (83) 2108-3051

Unidade Regional - Paraná

End.: Rua Marechal Deodoro, n° 555, 5º andar, Prédio Ministério da Fazenda

Curitiba/PR - CEP: 80.020-911

Tel.: (41) 3320-8385 / (41) 3320-8386

Fax: (41) 3224-8468

Unidade Regional - Pernambuco

End.: Avenida Conde da Boa Vista, nº 800, Ed. Apolônio Sales, 10º andar - Boa Vista

Recife/PE - CEP: 50.060-004

Tel.: (81) 2138-0202/ (81) 3138-0203

Unidade Regional - Piauí

End.: Praça Marechal Deodoro, s/nº, Ed. Ministério da Fazenda, 2º andar

Teresina/PI - CEP: 64.000-160

Tel.: (86) 4009-4853 / (86) 3215-8131

Unidade Regional - Rio de Janeiro

End.: Avenida Presidente Antônio Carlos, nº 375, Ed. Palácio da Fazenda, 7º andar, Sala 711 - Centro

Rio de Janeiro/RJ - CEP: 20.020-010

Tel.: (21) 3805-3700 / 3805-3702 / 3805-3707

Unidade Regional - Rio Grande do Norte

End.: Av. Hermes da Fonseca, 774, Tirol, Natal/RN

CEP: 59020-095

Tel.: (84) 3343-4732/ (84) 3343-4740/ (84) 3343-4747

Unidade Regional - Rio Grande do Sul

End.: Avenida Loureiro da Silva, nº 445, Ed. Ministério da Fazenda, 7° andar, Sala 704

Porto Alegre/RS - CEP: 90.013-900

Tel.: (51) 3455-2782 / (51) 3455-2770 / (51) 3455-2771

Unidade Regional - Rondônia

End.: Avenida Calama, nº 3.775 - Bairro da Embratel

Porto Velho/RO - CEP: 76.820-781

Tel.: (69) 2181-8251/ (69) 2181-8261 / (69) 2181-8263

Unidade Regional - Roraima

End.: Avenida Capitão Ene Garcez, nº 1.024 - São Francisco

Boa Vista/RR - CEP: 69.305-135

Tel.: (95) 3212-5220 (Gabinete) / (95) 3212-5229 (Apoio) / (95) 3212-5223 (NAP)

Unidade Regional - Santa Catarina

End.: R. Conselheiro Mafra, 784, Ático - Ed. Galaxy, Centro, Florianópolis/SC

CEP: 88.010-002

Tel.: (48) 3821-2145 / (48) 3821-2147

Unidade Regional - São Paulo

End.: Avenida Prestes Maia, nº 733, 14º andar, Sala 1403 - Centro

São Paulo/SP - CEP: 01.031-001

Tel.: (11) 2113-2501 / (11) 2113-2503 (11) 2113-2996 (Gabinete)

Unidade Regional - Sergipe

End.: Praça Graccho Cardoso, nº 44 - Bairro São José

Aracaju/SE - CEP: 49.015-180

Tel.: (79) 3214-3156 / (79) 3214-5509 / (79) 3214-3855

Unidade Regional - Tocantins

End.: Quadra 103 Norte, Rua NO 05, Lote 13, Ed. Ranzi - Salas 3, 5 e7 - Centro

Palmas/TO - CEP: 77.001-020

Tel.: (63) 3232-9350 (Geral) / (63) 3232-9354 (NAP) / (63) 3232-9360 (Gabinete)

ANEXO VIII DO TERMO DE REFERÊNCIA

MODELO DA PROPOSTA DE PREÇOS

A planilha a ser utilizada pelas proponentes para apresentação suas propostas está disponível no sítio eletrônico da CGU: http://www.cgu.gov.br/sobre/licitacoes-e-contratos/licitacoes/tipos/pregao .

Documento assinado eletronicamente por **GUSTAVO TOMAS COSTA**, **Auditor Federal de Finanças e Controle**, em 17/05/2018, às 11:03, conforme horário oficial de Brasília, com fundamento no art. 6º, §1º, do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **BIANCA CRISTINA LESSA ENDERS**, **Auditor Federal de Finanças e Controle**, em 17/05/2018, às 11:13, conforme horário oficial de Brasília, com fundamento no art. 6º, §1º, do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **GUSTAVO MOURA DE SOUSA**, **Integrante Requisitante**, em 21/05/2018, às 13:34, conforme horário oficial de Brasília, com fundamento no art. 6º, §1º, do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **ANTONIO MAROYSIO DOS SANTOS CARNEIRO**, **Coordenador-Geral de Infraestrutura Tecnológica**, em 24/05/2018, às 10:42, conforme horário oficial de Brasília, com fundamento no art. 6º, §1º, do Decreto nº 8.539, de 08 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.cgu.gov.br/conferir informando o código verificador 0724401 e o código CRC 21BB2863