1. Definição do Objeto

1.1 Registro de preços para eventual aquisição de ativos de rede (*hardware* e *software*) para modernização da rede de dados do Tribunal Superior do Trabalho, conforme condições abaixo e especificações constantes no Anexo I.

GRUPO ÚNICO				
Item	**Especificação**	**Unidade**	**Quantidade a Registrar**	**Pedido Mínimo**
01	*Switch Core* Tipo 1	Equipamento	2	1
Código CATMAT: 393273				
02	*Switch Core* Tipo 2	Equipamento	12	1
Código CATMAT: 393273				
03	*Switch* Acesso Tipo 1	Equipamento	3	1
Código CATMAT: 393274				
04	*Switch* Acesso Tipo 2	Equipamento	40	5
Código CATMAT: 393274				
05	*Switch* Acesso Tipo 3	Equipamento	110	10
Código CATMAT: 393274				
06	*Transceiver 10G SFP+ SR4*	Componente	882	2
Código CATMAT: 150812				
07	*Transceiver 40G QSFP+*, para distância de, no mínimo, 300m	Componente	8	2
Código CATMAT: 150812				
08	*Transceiver 40G QSFP+, SR4*	Componente	104	2
Código CATMAT: 150812				
09	*Transceiver 40G QSFP+*, para distância de, no mínimo, 2km	Componente	8	2
Código CATMAT: 150812				
10	Cabo DAC 40G com 1 metro	Cabo	12	2
Código CATMAT: 31313				
11	Cabo DAC 40G com 5 metros.	Cabo	16	4
Código CATMAT: 31313				
12	*Software* de Gerência	Solução	1	1
Código CATSER:5673				
13	Serviço de instalação dos equipamentos e do *software* de gerenciamento	Un.	1	1
Código CATSER: 1988				
14	Treinamento Oficial	Aluno	10	2
Código CATMAT/CATSER: 3840				

2. Fundamentação da Contratação

2.1 **Motivação da Contratação**

2.1.1 A rede de comunicação de dados do Tribunal Superior do Trabalho é composta atualmente por aproximadamente 180 equipamentos de comunicação, todos do fabricante *CISCO SYSTEMS*. Tais equipamentos são responsáveis por prover conectividade e acesso a todos os serviços oferecidos pelo TST, tais como acesso aos sistemas informatizados, drives de rede, correio eletrônico, banco de dados, mensageria instantânea, telefonia, sistemas de coletores biométricos, rede *wireless*, acesso à Internet, sistema de automação predial, estações de trabalho, CFTV, entre outros.

2.1.2 Esses equipamentos, em sua grande maioria, foram adquiridos no ano de 2005, não sendo mais possível a contratação de serviços de suporte técnico e atualização, o que aumenta consideravelmente o risco de longos períodos de indisponibilidade decorrente de problemas técnicos e vulnerabilidades de segurança.

2.1.3 Adicionalmente os novos recursos disponíveis no mercado não podem ser incorporados à rede atual do TST em virtude da falta de atualização dos equipamentos.

2.2 **Objetivos a serem alcançados**

2.2.1 Substituição de todos os ativos de rede por equipamentos novos, em garantia e desenvolvimento pelos fabricantes;

2.2.2 Implantação de um novo sistema (*software*) de gestão da rede (com serviços de diagnóstico, atualização e análise de vulnerabilidade da rede);

2.2.3 Treinamento da equipe que administra os equipamentos nos novos equipamentos e sistema adquiridos.

2.3 **Benefícios diretos e indiretos resultantes da contratação**

2.3.1 Disponibilização de novos recursos aos usuários e administradores da rede;

2.3.2 Gestão mais rápida e eficiente da rede de computadores, através de sistema próprio desenvolvido pelo próprio fabricante dos equipamentos;

2.3.3 Possibilidade de melhorias de segurança, disponíveis nos equipamentos mais novos;

2.3.4 Redução de indisponibilidades decorrentes do fim da vida útil dos equipamentos atuais.

2.4 **Alinhamento entre a contratação e os planos estratégicos do TST e planos estratégicos de Tecnologia da Informação**

2.4.1 A contratação em questão está alinhada com o Plano Estratégico do TST 2015 a 2020 na perspectiva “Recursos”, Objetivo “Garantir a infraestrutura e o orçamento” e também com o Plano Estratégico de Tecnologia da Informação e Comunicação do TST (PETIC 2015 a 2020) na perspectiva “Pessoas e Infraestrutura”, Objetivo Estratégico “Garantir a infraestrutura de TIC”.

2.5 **Referência aos Estudos Preliminares de STIC realizados**

2.5.1 Os estudos que apontaram essa solução e esses procedimentos estão anexados ao processo administrativo que trata dessa proposta de aquisição.

2.6 **Relação entre a demanda prevista e a quantidade de cada item**

2.6.1 Atualmente a rede de dados do TST, que propomos substituir, nos dá a possiblidade de conectarmos, em portas físicas, 632 dispositivos no Data Center e 6456 dispositivos na camada de acesso (na camada de distribuição não são conectados diretamente equipamentos que não de comunicação).

2.6.2 De forma, a satisfazer a necessidade para modernização da rede, serão necessários:

ITEM	DESCRIÇÃO	QTDE
1	*Switch Core* Tipo 1.	2
2	*Switch Core* Tipo 2.	12
3	*Switch* Acesso Tipo 1.	3
4	*Switch* Acesso Tipo 2.	40
5	*Switch* Acesso Tipo 3.	110
6	*Transceiver 10G SFP+ SR4*	882
7	*Transceiver 40G QSFP+*, para distância de, no mínimo, 300m.	8
8	*Transceiver 40G QSFP+, SR4*	104
9	*Transceiver 40G QSFP+*, para distância de, no mínimo, 2km	8
10	Cabo DAC 40G com 1 metro.	12
11	Cabo DAC 40G com 5 metros.	16
12	*Software* de Gerência.	1
13	Serviço de Instalação dos Equipamentos e do *Software* de Gerenciamento	1
14	Treinamento Oficial (por pessoa).	10

2.6.3 O Treinamento será oferecido para até 10 (dez) analistas, sendo 5 (cinco) da Seção de Gerenciamento de Redes, responsável direta pela administração da rede de computadores e 5 (cinco) técnicos de outras áreas da CITEC e SETIN, responsável pela gestão de toda a Infraestrutura de TIC do TST.

2.7 **Soluções similares disponíveis em outros órgãos e no Portal do Software Público Brasileiro**

2.7.1 Por se tratar de aquisição de equipamento de infraestrutura de rede não há solução disponível em outros órgãos ou no portal do *software* público brasileiro.

2.8 **Análise do mercado de Tecnologia da Informação e Comunicação**

2.8.1 Recentemente o Supremo Tribunal Federal realizou contratação, através do pregão eletrônico, nº 81/2017, com equipamentos similares ao pretendido pelo TST.

2.8.2 O Tribunal Regional do Trabalho de 8ª Região publicou pregão, nº 67/2017, cujo objeto é a aquisição de ativos de rede (*switches LAN* e *SAN*), módulos, acessórios, serviços de instalação, transferência de conhecimento, suporte técnico on-site e garantia estendida de, no mínimo, 60 (sessenta) meses. Por ser uma contratação bastante complexa, uma vez que engloba toda a Justiça do Trabalho, teve que ser suspensa para que houvesse uma audiência pública sendo posteriormente revogada. No último dia 16/5/2018 foi publicado novo pregão, nº 24/2018, onde o TST também é partícipe.

2.9 **Natureza do objeto a ser contratado**

2.9.1 Trata-se de aquisição de equipamentos de comunicação de dados com serviços de instalação e suporte técnico em garantia. Os equipamentos são claramente especificados, com padrões de qualidade definidos, conhecidos pelo mercado, produzidos por diversos fabricantes e comercializados por inúmeras empresas, classificando-se assim como bens comuns.

2.10 **Justificativas para o parcelamento ou não da solução**

2.10.1 A solução não poderá ser parcelada, uma vez que se trata de um conjunto que deverá ser substituído integralmente objetivando a redução de efeitos colaterais decorrentes da alteração de ambiente crítico e de grande impacto no trabalho do órgão.

2.10.2 Caso haja restrição orçamentária avaliaremos a melhor forma de realizar a substituição a partir da adesão à ata de registro de preços gerada.

2.11 **Forma de adjudicação do objeto**

2.11.1 A adjudicação do objeto será global, de forma que os produtos formem um conjunto único, compatíveis em marca e modelo e projeto.

2.11.2 Os itens necessários para suprir a necessidade de utilizar uma solução de rede com suporte apropriado devem ser agrupados para formação de um único lote para licitação, pois todos os bens e serviços estão intrinsecamente relacionados. Tal organização permite ganhos quanto à instalação, configuração, operacionalização e treinamento em toda a solução.

2.11.3 A divisão de itens como, por exemplo, da solução de rede central e de rede de acesso, pode resultar na compra de soluções incompatíveis, o que acarretaria em prejuízo ao Tribunal.

2.12 **Modalidade e tipo de licitação**

2.12.1 Propomos a realização de Pregão Eletrônico para Registro de Preços, com o objetivo de dividir a aquisição em dois períodos orçamentários.

2.13 **Impacto ambiental decorrente da contratação**

2.13.1 Os equipamentos atuais serão descartados ou doados de acordo com a legislação ambiental vigente. Não haverá impacto ambiental decorrente da contratação.

3. Modelo de execução e gestão do contrato

3.1 **Deveres e responsabilidades do Contratante**

3.1.1 Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações contratuais, inclusive permitir o livre acesso dos técnicos da Contratada às dependências do Contratante para a realização das atividades relacionadas à execução do contrato.

3.1.2 Promover os pagamentos em moeda corrente nacional, mediante depósito na conta bancária indicada pela Contratada, após o ateste da Nota Fiscal.

3.1.3 Fornecer atestados de capacidade técnica quando solicitado, desde que atendidas às obrigações contratuais.

3.1.4 Após a assinatura do contrato, o Contratante designará, formalmente, servidor ou comissão de servidores para exercerem o acompanhamento e fiscalização da execução contratual.

3.2 **Deveres e responsabilidades da Contratada**

3.2.1 Entregar o objeto e executar os serviços descritos no contrato nos prazos máximos nele determinados.

3.2.2 Atender prontamente às solicitações da fiscalização do contrato, inerentes ao objeto, sem qualquer ônus adicional para o órgão Contratante.

3.2.3 Cumprir todos os requisitos descritos no contrato, responsabilizando-se pelas despesas de deslocamento de técnicos, diárias, hospedagem e demais gastos relacionados com a equipe técnica, sem qualquer custo adicional para o Contratante.

3.2.4 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, as partes do objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes dos materiais empregados ou da execução dos serviços.

3.2.5 Responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez inexistir, no caso, vínculo empregatício deles com o Contratante.

3.2.6 Responder integralmente por perdas e danos que vier a causar ao Contratante ou a terceiros em razão de ação ou omissão dolosa ou culposa, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

3.2.7 Respeitar o sistema de segurança do Contratante e fornecer todas as informações solicitadas por ele, relativas ao cumprimento do objeto.

3.2.8 Acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades.

3.2.9 Guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do Contratante, sendo vedada, à Contratada, sua cessão, locação ou venda a terceiros.

3.2.10 Utilizar padrões definidos em conjunto com o Tribunal (nomenclaturas, metodologias, etc.).

3.2.11 Observar os requisitos de segurança da informação elencados no ANEXO II deste termo.

3.2.12 Comprovar a quitação dos tributos de importação referentes aos produtos, conforme disposto no Decreto nº 7.174/2010, art. 3º, inc. III, da seguinte forma:

3.2.12.1 Caso os produtos entregues sejam importados e a Contratada for a importadora, a comprovação poderá ser feita por meio da apresentação dos seguintes documentos, sob pena de rescisão contratual e multa:

a) Comprovante de Importação emitido no Siscomex quando a Declaração de Importação – DI é desembaraçada;

b) Última versão do extrato da Declaração de Importação.

3.2.12.2 Os bens fornecidos devem estar descritos na DI de forma a permitir a identificação precisa, constando marca, modelo e, se possível, nº de série.

3.2.12.3 Caso o produto entregue não seja importado deverá ser apresentada, no momento da entrega, uma declaração da Contratada atestando essa situação.

3.2.12.4 A declaração deverá ser apresentada mesmo para as empresas que participaram da licitação utilizando-se da preferência de que trata o art. 3º da Lei 8.248/91.

3.2.12.5 Caso o produto entregue seja importado, mas se a Contratada não for a titular da obrigação tributária correspondente, a contratada deverá comprovar, no momento da entrega, a aquisição do produto importado pelo contratado não importador, junto ao seu fornecedor, de modo a afastar sua responsabilidade pelos tributos de importação, considerando não ser sujeito passivo tributário.

3.3 Especificação técnica do objeto

3.3.1 A especificação técnica dos objetos desta licitação está consolidada no Anexo I.

3.4 Observações gerais a respeito do objeto

3.4.1 Os números relacionados na coluna “Quantidade a Registrar” da Tabela 1, correspondem aos totais de unidades dos itens a serem ofertados, de forma a atender às necessidades levantadas e à padronização técnica, sob pena da desclassificação.

3.4.2 O preço final deverá incluir todas as despesas referentes ao frete, às embalagens, aos tributos e aos demais encargos indispensáveis ao perfeito cumprimento das obrigações decorrentes do contrato.

3.4.3 A proposta deverá especificar, quando cabíveis: marca, modelo, data de fabricação, data de validade, fabricante, custos unitários e totais e, se possível, outras referências que bem identifiquem o objeto cotado.

3.4.4 O objeto deverá ser entregue no Tribunal Superior do Trabalho – SAFS – Quadra 8, Lote 1, Subsolo, Seção de Controle de Patrimonial – SCPAT, Brasília/DF, CEP 70070-600 – Tel: (61) 3043-4097.

3.4.5 Os materiais deverão ser acondicionados em embalagens lacradas, com a identificação do produto.

3.5 Prazos de execução

3.5.1 Em até 10 (dez dias) a partir da assinatura do contrato deverá ocorrer a reunião de alinhamento de expectativas, onde serão detalhados os cronogramas (a previsão) de entrega, apresentados os gerentes do projeto e a equipe técnica da contratada, bem como iniciado o projeto de substituição dos equipamentos atuais pelos recém-adquiridos.

3.5.2 A entrega total dos equipamentos e *software*, objeto da ordem de fornecimento, descritos nos itens de 1 a 12, deverá ocorrer em até 60 (sessenta) dias corridos e contados após a assinatura do contrato.

3.5.3 O recebimento provisório dos itens 1 a 12 será emitido em até 5 (cinco) dias corridos e contados a partir da entrega dos equipamentos e do *software* de gerência;

3.5.4 O recebimento definitivo dos itens de 1 a 12 será emitido em até 15 (quinze) dias corridos e contados após a data do recebimento provisório;

3.5.5 O pagamento relativo aos itens 1 a 12 será feito em até 10 (dez) dias úteis após a emissão do termo de recebimento definitivo;

3.5.6 O prazo de garantia técnica dos itens 1 a 12 deverá ser de, no mínimo, 60 (sessenta) meses após a emissão do termo de recebimento definitivo dos equipamentos;

3.5.7 A primeira entrega do item 13, que trata do serviço de instalação referente aos itens 1 a 12 deverão ocorrer em até 30 (trinta) dias corridos e contados após o recebimento definitivo dos respectivos objetos e *softwares*;

3.5.8 O recebimento do item 13 será emitido pela equipe técnica da CITEC em até 5 (cinco) dias corridos após a verificação de que todos os respectivos equipamentos e *software* foram instalados, testados e estão em conformidade conforme proposto;

3.5.9 O pagamento referente ao item 13 ocorrerá em até 10 (dez) dias úteis após o seu recebimento;

3.5.10 O início da contagem de prazo de suporte técnico para os itens 1 e 2 se inicia após o recebimento do item 13;

3.5.11 O prazo de entrega do item 14, treinamento oficial, será de até 60 (sessenta) dias corridos e contados após a assinatura do Contrato;

3.5.12 O recebimento referente ao item 14, treinamento oficial, será de até 5 (cinco) dias corridos da finalização do curso após análise da avaliação por parte do TST e verificação de atendimentos às demais condições contratuais;

3.5.13 O pagamento referente ao item 14, treinamento oficial, ocorrerá em até 10 (dez) dias úteis após a emissão do recebimento definitivo do serviço de treinamento.

3.5.14 Na contagem dos prazos previstos neste documento, excluir-se-á o dia de início e incluir-se-á o dia do vencimento. Só se iniciam e vencem os prazos em dias úteis e de expediente no Tribunal Superior do Trabalho.

3.5.15 Havendo pedido de prorrogação do prazo de entrega, este somente será concedido nas hipóteses previstas no Art. 57, §1°, da Lei nº 8.666/93, em caráter excepcional e sem efeito suspensivo, e deverá ser encaminhado por escrito, com antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada.

3.5.16 Em casos excepcionais, autorizados pelo Contratante, o documento comprobatório do alegado poderá acompanhar a entrega do produto.

3.6 **Garantia on-site do objeto**

3.6.1 A garantia técnica será aquela, usualmente fornecida pelo fabricante acrescida dos Níveis de Serviço Exigidos (NSE) e demais condições estabelecidas neste Estudo Técnico;

3.6.2 A garantia técnica para todos os equipamentos será de 60 (sessenta) meses.

3.6.3 A garantia visa restabelecer as condições normais de uso dos equipamentos incluindo a substituição de peças, componentes ou dos switches como um todo se necessário. Os custos incorridos na execução da garantia serão exclusivos da Contratada, sem ônus adicional para o TST;

3.6.4 A garantia técnica deverá ser realizada durante todo o período pela própria Contratada, ou diretamente com o fabricante dos equipamentos, a fim de que sejam mantidos válidos todos os direitos oriundos da garantia, excluindo-se a possibilidade de falta de cobertura por manutenções realizadas sem a habilidade técnica necessária ou indisponibilidade de equipamentos e peças;

3.6.5 O modelo de prestação da garantia técnica será por solicitação, ou seja, a Contratada receberá da CITEC a solicitação para o atendimento de garantia conforme as severidades especificadas neste documento;

3.6.6 A Contratada deverá apresentar comprovação formal da aquisição da garantia técnica junto ao Fabricante, abrangendo todos os equipamentos e *softwares* da solução;

3.6.7 As solicitações já existentes quando do final do período de garantia técnica deverão ser devidamente atendidas, considerados inclusive os prazos estipulados neste documento.

3.6.8 O serviço de suporte técnico será realizado presencialmente, quando solicitado pela Contratada, por intermédio de correio eletrônico (e-mail), por ferramentas do tipo chat e por telefone, todos em língua portuguesa, no Brasil, em regime 24 x 7 (vinte e quatro por sete) para os equipamentos dos itens 1 e 2 e 8 x 5 (oito por cinco) para os equipamentos dos itens 3, 4, 5 e 12;

3.6.9 Os itens acessórios: 6, 7, 8, 9, 10 e 11, deverão assumir os níveis de suporte dos equipamentos onde estiverem instalados/conectados.

3.6.10 O serviço de garantia consistirá na reparação das eventuais falhas dos equipamentos, consultas referentes à configuração, diagnóstico, ajustes e substituição de peças, componentes ou até mesmo equipamentos inteiros que se apresentem defeituosos e de acordo com manuais e normas técnicas específicas para os equipamentos.

3.6.11 O suporte técnico para eventos, incidentes e problemas quanto à operação da solução serão pautados por Níveis de Serviço Exigidos (NSE) previamente definidos neste estudo. Serão considerados para efeitos dos níveis exigidos:

I. **Prazo de Atendimento**: tempo decorrido entre a abertura do chamado técnico efetuado pela equipe da CITEC na Central de Atendimento da Contratada e o efetivo início dos trabalhos de suporte;

II. **Prazo de Solução Definitiva**: tempo decorrido entre a abertura do chamado técnico efetuado pela equipe da CITEC na Central de Atendimento da Contratada e a efetiva recolocação do(s) equipamento(s) em pleno estado de funcionamento;

III. A contagem do **prazo de atendimento** e a **solução definitiva** de cada chamado serão a partir da abertura do chamado técnico na Central de Atendimento disponibilizada pela Contratada, até o momento da comunicação da solução definitiva do problema e aceite pela equipe técnica da CITEC.

3.6.12 Na abertura do chamado técnico do equipamento junto à Central de Atendimento serão fornecidas, no mínimo, as seguintes informações:

I. Modelo e número de série do equipamento;

II. Problema observado;

III. Contato do profissional do TST responsável pela solicitação do atendimento;

IV. Nível de severidade do chamado.

3.6.13 Os Níveis de Serviços Exigidos (NSE), para os itens 1, 2 e 12, serão classificados conforme as severidades a seguir:

I. **Severidade ALTA**: esse nível de severidade é aplicado quando há a indisponibilidade do uso do(s) equipamento(s) ou do *software*. Para este nível de severidade o prazo de atendimento será de 2 (duas) horas e de 4 (quatro) horas para a solução definitiva;

II. **Severidade MÉDIA**: esse nível de severidade é aplicado quando há falha, simultânea ou não do uso do(s) equipamento(s) ou do *software*, estando ainda disponíveis, porém apresentando problemas. Para este nível de severidade o prazo de atendimento será de 4 (quatro) horas e de 12 (doze) horas para a solução definitiva;

III. **Severidade BAIXA**: esse nível de severidade é aplicado quando o equipamento ou o *software* apresentar desempenho degradado ou sinal de alerta, mas sem afetar o uso dos sistemas. Para este nível de severidade o prazo de atendimento será de 8 (oito) horas e de 24 (vinte e quatro) horas para a solução definitiva;

IV. **INFORMAÇÃO**: Solicitação de informações relacionadas à instalação, configuração ou recursos do equipamento e/ou *software*. Início de atendimento será de 24 (vinte e quatro) horas e de 10 (dez) dias úteis para a solução definitiva.

3.6.14 Para os itens 3, 4 e 5, os equipamentos deverão ser substituídos em até 48 horas a partir da comunicação do defeito.

I. Não serão admitidas tentativas de reparo dos equipamentos defeituosos (itens 3, 4 e 5).

3.6.15 O atendimento aos chamados técnicos de severidade ALTA deverá ser realizado on-site, quando solicitado pela equipe técnica da CITEC e não

poderá ser interrompido até o completo restabelecimento do serviço, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados. Neste caso, não poderão acarretar custos adicionais ao TST. A interrupção do suporte de um chamado técnico desse tipo de severidade pela Contratada, e que não tenha sido previamente autorizado pela equipe da CITEC poderá ensejar em aplicação de penalidades previstas;

3.6.16 Os chamados técnicos classificados com severidade MÉDIA, quando não solucionados no prazo definido, poderão ser automaticamente escolados para a severidade ALTA, sendo que os prazos de atendimento e solução definitiva do problema, bem como penalidades previstas, serão automaticamente ajustados para o novo nível. A interrupção do suporte de um chamado técnico desse tipo de severidade pela Contratada, e que não tenha sido previamente autorizado pela equipe técnica da CITEC, poderá ensejar em aplicação de penalidades previstas;

3.6.17 Os chamados técnicos terão origem em decorrência de qualquer problema detectado pela equipe técnica da CITEC e que esteja prejudicando o pleno funcionamento do equipamento, inclusive problemas relacionados à instalação, configuração ou mau funcionamento;

3.6.18 Ao final de cada atendimento solicitado, troca de equipamento provisório ou definitivo, configuração, manutenção ou instalação, a Contratada emitirá um relatório de atendimento com todas as informações relevantes ao serviço solicitado;

3.6.19 Após a conclusão do suporte a Contratada comunicará o fato à equipe técnica da CITEC e solicitará autorização para o fechamento do chamado. Caso a equipe técnica da CITEC não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela Contratada. Nesse caso a equipe técnica da CITEC fornecerá as pendências relativas ao chamado aberto;

3.6.20 Por necessidade excepcional de serviço, a equipe técnica da CITEC também poderá solicitar a escalação de chamado para níveis superiores de severidade. Nesse caso, a escalação deverá ser justificada e os prazos dos chamados técnicos passarão a contar do início novamente;

3.6.21 Sempre que houve quebra dos níveis de serviço exigidos, o TST emitirá notificação à Contratada, que terá o prazo de, no máximo, 5 (cinco) dias corridos e contados a partir do recebimento da notificação para apresentar as justificativas para as falhas verificadas;

3.6.22 Caso não haja manifestação dentro desse prazo ou caso o TST entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme o nível de serviço transgredido;

3.6.23 A Contratante poderá abrir chamados de manutenção diretamente no Fabricante, sem a necessidade de consulta prévia e/ou qualquer liberação por parte da Contratada;

3.6.24 Não haverá limite para abertura de chamados, sejam de dúvidas/configurações e/ou resolução de problemas de *hardware* ou *software*;

3.6.25 Deverá ser garantido ao Contratante o acesso ao site do fabricante dos equipamentos e *softwares*. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários, relacionados aos equipamentos e *softwares* especificados, além de permitir downloads de quaisquer atualizações de *software* ou documentação do produto;

3.6.26 Caberá à Contratada apresentar soluções definitivas para os problemas apresentados, inclusive problemas relacionados com instalação, configuração e atualização, dentro dos prazos e condições estabelecidas neste documento;

3.6.27 A Contratada informará o número do chamado técnico no ato da comunicação efetuada pela equipe técnica da CITEC que servirá de referência para acompanhamento, inclusive após o encerramento do chamado. O número do chamado deverá ser informado dentro do prazo para atendimento estabelecido nos níveis de serviço exigidos (NSE);

3.6.28 O fornecedor deverá assegurar a garantia dos equipamentos, seja por meio da rede mantida pelo próprio fabricante ou por meio de rede por ele credenciada, sendo, em todo caso, capaz de atender no local de entrega dos equipamentos com, no mínimo, um estabelecimento técnico;

3.6.29 O serviço de garantia on-site, poderá utilizar apenas peças e componentes originais salvo nos casos fundamentados por escrito e aceitos pelo Contratante;

3.6.30 O término do reparo do equipamento não poderá ultrapassar o prazo previsto, caso contrário, a Contratada deverá providenciar a colocação de equipamento equivalente ou de superior configuração, em perfeitas condições de uso, como backup, até que seja sanado o defeito do equipamento. O prazo máximo para o backup permanecer no Tribunal não deverá ser superior a 30 (trinta) dias;

3.6.31 A abertura de chamados será efetuada por correio eletrônico e por telefone 0800 ou com número de DDD igual ao da localidade do contratante. Em ambos os casos, o atendimento deve ser efetuado em Língua Portuguesa;

3.6.32 Na abertura do chamado, a Contratada deverá fornecer um número de registro para acompanhamento de cada equipamento;

3.6.33 O início de atendimento e da resolução do serviço de garantia será a hora da comunicação feita pelo Contratante à Contratada, conforme sistema de registro do próprio do solicitante.

3.7 Garantia contratual

3.7.1 Para segurança do Contratante quanto ao cumprimento das obrigações contratuais, a Contratada deverá optar, no montante de 5% (cinco por cento) do valor total do contrato, por uma das seguintes modalidades de garantia:

I. Caução em dinheiro ou em títulos da dívida pública, devendo estes terem sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;

II. Seguro-garantia;

III. Fiança bancária.

3.7.2 A Contratada deverá providenciar a garantia contratual impreterivelmente em dez dias úteis contados da assinatura do contrato, prorrogáveis por igual período a critério do Contratante desde que solicitado dentro do prazo inicial, sob pena de ser-lhe imputada multa.

3.7.3 É de inteira responsabilidade da Contratada a renovação da garantia prestada, quando couber, estando sua liberação condicionada ao término das obrigações contratuais com o TST.

3.8 **Vigência**

3.8.1 O contrato terá vigência de 60 (sessenta) meses contados a partir do recebimento definitivo.

3.9 **Fiscalização**

3.9.1 Os produtos e serviços objetos desta contratação serão fiscalizados por servidor ou comissão de servidores do Contratante, doravante denominados Fiscalização, que terá autoridade para exercer toda e qualquer ação de orientação geral, controle e fiscalização da execução contratual.

3.9.2 À Fiscalização compete, entre outras atribuições:

I. Solicitar à Contratada e seus prepostos, ou obter da Administração, tempestivamente, todas as providências necessárias ao bom andamento do contrato e anexar aos autos do processo correspondente cópia dos documentos escritos que comprovem essas solicitações de providências;

II. Manter organizado e atualizado um sistema de controle em que se registrem as ocorrências ou os serviços descritos de forma analítica;

III. Acompanhar e atestar a prestação dos serviços contratados e indicar a ocorrência de inconformidade desses serviços ou não cumprimento do contrato;

IV. Encaminhar à Secretaria de Administração os documentos para exame e deliberação sobre a possível aplicação de sanções administrativas.

3.9.3 A ação da Fiscalização não exonera a Contratada de suas responsabilidades contratuais.

3.10 **Recebimento do objeto**

3.10.1 Em conformidade com os artigos 73 a 76 da Lei n.º 8.666/93, o objeto deste contrato será aceito:

I. Provisoriamente, mediante recibo, em, no máximo, 5 (cinco) dias depois de efetuada a entrega do objeto, para efeito de posterior verificação de sua conformidade;

II. Definitivamente, mediante Termo de Recebimento Definitivo, em até 15 (quinze) dias úteis.

3.10.2 O objeto deverá ser acondicionado em embalagem original lacrada, com a identificação do produto, fazendo constar sua descrição e incluindo o nome do fabricante, a marca ou modelo do material de acordo com suas características.

3.10.3 Por ocasião da entrega do objeto será requerido o fornecimento da documentação de suporte técnico e manutenção em garantia, contendo as informações necessárias para abertura dos chamados por telefone e por correio eletrônico (códigos de acesso, números de telefone, endereços de correio eletrônico, códigos de identificação do cliente, etc.).

3.10.4 Após o recebimento provisório, a fiscalização avaliará as características do objeto, identificando eventuais problemas. Estando em conformidade, será efetuado o recebimento definitivo.

3.10.5 Se, após o aceite provisório, constatar-se que o objeto foi entregue em desacordo com este contrato ou com a proposta, com incorreção, ou incompleto, serão interrompidos os prazos de recebimento e suspenso o pagamento, após a notificação por escrito à Contratada e até que seja sanada a situação.

3.10.6 Os objetos entregues em desacordo com o especificado neste termo de referência, no instrumento convocatório, no contrato ou com defeito serão rejeitados parcial ou totalmente, conforme o caso, e a Contratada será obrigada a substituí-los dentro do prazo contratual, sob pena de se considerar atraso na entrega.

3.10.7 A Contratada ficará obrigada a trocar, a suas expensas, o material que vier a ser recusado.

3.10.8 A Contratada deverá retirar o material recusado no momento da entrega do material correto. O Tribunal Superior do Trabalho não se responsabilizará por qualquer dano ou prejuízo que venha a ocorrer após esse prazo.

3.10.9 A Administração poderá dar a destinação que julgar conveniente ao material abandonado em suas dependências.

3.10.10 A Contratada deverá entregar todo o material discriminado na nota de empenho, não havendo pagamento em caso de entrega parcial até que ocorra o adimplemento da obrigação.

3.10.11 Independentemente da aceitação, a Contratada garantirá a qualidade de cada unidade do produto fornecido pelo prazo estabelecido nas especificações, obrigando-se a reparar aquela que apresentar defeito no prazo estabelecido pelo Contratante.

3.10.12 O aceite provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança do serviço, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou por este instrumento.

3.11 **Pagamento**

3.11.1 O pagamento será efetuado em moeda corrente nacional, mediante depósito na conta bancária indicada pela Contratada, em até 10 dias úteis após o

recebimento definitivo do objeto e condicionado à apresentação das notas fiscais/faturas, devidamente, atestadas pela fiscalização.

3.11.2 As notas fiscais e os documentos exigidos no edital e no contrato, para fins de liquidação e pagamento das despesas, deverão ser entregues, exclusivamente, na Coordenadoria de Material e Logística, situada no SAFS, quadra 8, lote 1, Bloco A, Subsolo, Brasília-DF.

3.11.3 Serão retidos na fonte os tributos elencados nas disposições determinadas pelos órgãos fiscais e fazendários, em conformidade com as instruções normativas vigentes.

3.12 **Sanções**

3.12.1 Fundamentado no artigo 28 do Decreto n.º 5.450/2005, ficará impedido de licitar e contratar com a União e será descredenciado no SICAF, pelo prazo de até 5 (cinco) anos, garantido o direito à ampla defesa, sem prejuízo das multas previstas neste edital e das demais cominações legais, aquele que:

3.12.2 Não assinar a Ata de Registro de Preços/Receber a Nota de Empenho;

3.12.3 Deixar de entregar documentação exigida neste edital;

3.12.4 Apresentar documentação falsa;

3.12.5 Ensejar o retardamento da execução do objeto;

3.12.6 Não mantiver a proposta;

3.12.7 Falhar ou fraudar na execução contratual;

3.12.8 Comportar-se de modo inidôneo;

3.12.9 Fizer declaração falsa;

3.12.10 Cometer fraude fiscal;

3.12.11 No caso de atraso injustificado ou inexecução total ou parcial do compromisso assumido com o TST, as sanções administrativas aplicadas à Contratada serão:

3.12.11.1 Advertência;

3.12.11.2 Multa de:

3.12.11.2.1 1% (um por cento) ao dia sobre o valor referente ao respectivo item, no caso de atraso injustificado para a entrega dos **equipamentos e do *software* de gerenciamento (itens 1 a 12)**, limitado à incidência de 30 (trinta) dias, quando será considerada a inexecução do contrato;

3.12.11.2.2 1% (um por cento) ao dia sobre o valor referente aos itens a serem instalados, no caso de atraso injustificado para conclusão do **Serviço de Instalação dos Equipamentos e do *Software* de Gerenciamento**, limitado à incidência de 30 (trinta) dias, quando será considerada a inexecução do contrato;

3.12.11.2.3 Para os itens 3, 4, 5, 6, 7, 8, 9, 10 e 11, 2% (dois por cento)

ao dia sobre o valor do item, no caso de atraso injustificado para **substituição do equipamento, dentro do período de garantia**;

3.12.11.2.4 Para os itens 1 e 2, 2% (dois por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados técnicos abertos com nível de **Severidade ALTA**;

3.12.11.2.5 Para os itens 1 e 2, 1% (um por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados técnicos abertos com nível de **Severidade MÉDIA**;

3.12.11.2.6 Para os itens 1 e 2, 0,5% (meio por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados técnicos abertos com nível de **Severidade BAIXA**;

3.12.11.2.7 0,5% (meio por cento) ao dia sobre o valor do item substituído temporariamente por equipamento *backup* e não reestabelecido dentro do prazo estipulado (violação do item 3.6.30).

3.12.11.3 Suspensão temporária de participar de licitações e impedimento de contratar com o Tribunal Superior do Trabalho;

3.12.11.4 Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

3.12.12 A Contratada deverá justificar fundamentada, prévia e formalmente qualquer ocorrência que a leve a descumprir os deveres estabelecidos neste Termo. A aceitação da justificativa ficará a critério do Contratante.

3.12.13 As multas porventura aplicadas serão descontadas dos pagamentos devidos pelo Contratante, da garantia ofertada ou cobradas diretamente da Contratada, amigável ou judicialmente, e poderão ser aplicadas cumulativamente às demais sanções previstas nesta cláusula.

3.12.14 As penalidades serão obrigatoriamente registradas no SICAF e sua aplicação será precedida da concessão da oportunidade de ampla defesa para o adjudicatário, na forma da lei.

3.12.15 Os prazos de adimplemento das obrigações contratadas admitem prorrogação nos casos e condições especificados no § 1º do art. 57 da Lei 8.666/93, em caráter excepcional, sem efeito suspensivo, devendo a solicitação ser encaminhada por escrito, com antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada.

3.12.16 Eventual pedido de prorrogação deverá ser encaminhado para o seguinte endereço: Seção de Gestão de Contratos, Tribunal Superior do Trabalho,

SAFS, quadra 08, lote 1, Bloco A, térreo, sala T-18, Brasília-DF, CEP 70.070-943, fones: (061) 3043-4165, (061) 3043-7570 e-mail: sgcon@tst.jus.br.

3.12.17 Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério do Contratante.

3.13 **Demais disposições**

3.13.1 É de responsabilidade da Contratada o conhecimento das características do material relacionado no objeto desta licitação.

3.13.2 O TST não aceitará, sob nenhum pretexto, a transferência de responsabilidade da Contratada para terceiros, sejam fabricantes, representantes ou quaisquer outros.

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

Requisitos Tecnológicos (hardware e software) – *Todos os itens*	
ID	**Descrição**
R.HS.01	Todos os equipamentos descritos nos requisitos tecnológicos, bem como os *transceivers* descritos no item 2.5, devem ser do mesmo fabricante de forma a manter a compatibilidade e interoperabilidades entre estes;
R.HS.02	Todos os equipamentos e *softwares* que compõem a Solução de Gerenciamento devem ser homologados pelo Fabricante e suportados pela Contratada, de maneira a garantir a padronização e interoperabilidade entre todos os componentes;
R.HS.03	A Solução de Gerenciamento deverá ter a capacidade de gerenciamento de até 5.000 dispositivos concorrentes;
R.HS.04	O licenciamento da Solução de Gerenciamento deve viger durante 60 (sessenta) meses;
R.HS.05	É de responsabilidade da Contratada todos os ajustes dos parâmetros de QoS para o correto funcionamento do serviço de voz sobre IP na rede do TST;
R.HS.06	A Licitante, junto com a proposta, deverá apresentar documentação técnica do equipamento ofertado, com o detalhamento de todas as especificações e requisitos que são objeto da Contratação.

Requisitos Tecnológicos (hardware e software) – *Switch Core Tipo 1*	
ID	**Descrição**
R.HS.C1.01	O equipamento deve ser novo e estar em linha de produção, ou seja, com suporte ativo e ciclo de vida garantido pelo fabricante por, no mínimo, 5 (cinco) anos;
R.HS.C1.02	O equipamento deve possuir, no mínimo, 24 (vinte e quatro) portas QSFP+ 40*GbE* em modo *wirespeed* e *non-blocking*, compatíveis com: • *Transceivers* padrões 40GBase-SR4 e 40GBase-LR4; • Cabos QSFP+ *Direct Attach Cable* (DAC), conforme a especificação 40GBase-CR4. Não é permitida a utilização conversores externos;
R.HS.C1.03	Possuir uma porta de console com conector RJ-45 ou DB9 macho;
R.HS.C1.04	Possuir uma porta 10/100/1000 ou 1G/10G com conector RJ-45 para gerência *out-of-band* do equipamento;
R.HS.C1.05	Possuir na configuração ofertada fontes de alimentação redundantes e *hot-swappable*, onde a falha de uma fonte não deve implicar na parada de nenhuma função do equipamento;
R.HS.C1.06	As fontes de alimentação e a bandeja de ventiladores devem ser do tipo *hot-swappable*, devendo poder ser substituída sem que seja necessário desligar o equipamento, interromper seu funcionamento ou ter que retirar qualquer módulo;
R.HS.C1.07	Possuir capacidade de *switching* de, pelo menos, 2 Tbps;
R.HS.C1.08	Possuir taxa de encaminhamento de pacotes de no mínimo 1900 Mpps;
R.HS.C1.09	Implementar *switching* L2 e L3 localmente. O equipamento deve ser fornecido com todos os componentes necessários para esta finalidade;
R.HS.C1.10	Implementar roteamento estático com suporte a, no mínimo, 1000 (mil) rotas IPv4;

R.HS.C1.11	Implementar OSPF-v3 *full*, incluindo autenticação MD-5;
R.HS.C1.12	Implementar BGPv4;
R.HS.C1.13	Implementar roteamento IPv6;
R.HS.C1.14	Implementar agregação de *links* conforme padrão IEEE 802.3ad com, no mínimo, 24 grupos, permitindo até oito *links* agregados por grupo;
R.HS.C1.15	Implementar agregação de *links* conforme padrão IEEE 802.3ad com suporte a LACP;
R.HS.C1.16	Implementar agregação de *links* entre múltiplos *switches* (MLAG ou similar), possibilitando combinar a largura de banda de portas físicas pertencentes a *switches* físicos distintos;
R.HS.C1.17	Deve suportar o armazenamento de, no mínimo, 128.000 endereços MAC;
R.HS.C1.18	Implementar, no mínimo, 512 regras de ACL de saída (*egress ACLs*);
R.HS.C1.19	O equipamento deve implementar VRF (*Virtual Routing Forwarding*), MCE ou equivalente;
R.HS.C1.20	Implementar jumbo *frames* em todas as portas ofertadas, com suporte a pacotes de até 9000 *Bytes*;
R.HS.C1.21	Permitir a configuração de, no mínimo, 3965 VLANs;
R.HS.C1.22	Implementar protocolo *Virtual Router Redundancy Protocol – VRRP-v2* e *VRRP-v3* ou mecanismo similar de redundância de *default gateway*;
R.HS.C1.23	Implementar STP (*Spanning Tree Protocol*) de acordo com o IEEE 802.1d, RSTP (*Rapid Reconfiguration for Spanning Tree Protocol*) de acordo IEEE 802.1w e 802.1D e MSTP (*Multiple Instances of Spanning Tree Protocol*) de acordo com IEEE 802.1s;
R.HS.C1.24	Implementar PVST+ ou similar;
R.HS.C1.25	Implementar VLAN (*Virtual bridged Local Area Network*) e VLANs *Tagging* de acordo com IEEE 802.1Q;
R.HS.C1.26	Suportar autenticação baseada em MAC ou WEB;
R.HS.C1.27	Implementar QoS de acordo com IEEE 802.1p;
R.HS.C1.28	Implementar os algoritmos de gerenciamento de filas WRR (*Weighted Round Robin*) ou DWRR (*Deficit Weighted Round Robin*) ou WFW (*Weighted Fair Queuing*) e SP (*Strict Priority*) ou WRED (*Weighted Random Early Detection*) e SP (*Strict Priority*);
R.HS.C1.29	Suportar IGMPv2 ou superior e IGMP *Snooping* para controle de tráfego *multicast*;
R.HS.C1.30	Permitir a suspensão de recebimento de BPDUs (*Bridge Protocol Data Units*) caso a porta esteja colocada no modo *fast forwarding*, conforme previsto no padrão IEEE 802.1w. Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
R.HS.C1.31	Permitir o espelhamento do tráfego de entrada e saída de múltiplas portas do *switch* em uma única porta;
R.HS.C1.32	Implementar DHCP *Relay* permitindo a definição de pelo menos dois servidores DHCP;
R.HS.C1.33	Implementar DHCP *snooping* ou funcionalidade similar que permita o bloqueio de servidores DHCP não autorizados na rede;
R.HS.C1.34	Permitir a classificação e priorização de pacotes baseada em informações de camada 2, 3 e 4 do modelo OSI, para no mínimo: Endereço MAC, endereço IP, número de porta TCP ou UDP, valor do campo CoS (802.1p) e valor do

	campo ToS (com precedência IP e DSCP);
R.HS.C1.35	Permitir a configuração de, no mínimo, oito filas de prioridade por porta;
R.HS.C1.36	Permitir a limitação de endereços MAC por porta. Os endereços MAC podem ser aprendidos automaticamente ou configurados manualmente;
R.HS.C1.37	Possuir mecanismos para controle dos tráfegos de *broadcast*, *multicast* e *unknown-unicast* (ou funcionalidade similar para o controle de tráfego *unknown-unicast*) por porta. Deve ser possível especificar limites individuais para tráfego tolerável de *broadcast*, *multicast* e *unknown-unicast* em cada porta do *switch*;
R.HS.C1.38	Permitir a limitação de tráfego (*rate limiting*);
R.HS.C1.39	Implementar roteamento entre as VLANs internamente, sem a necessidade de equipamentos externos;
R.HS.C1.40	Implementar filtros baseados em protocolos e endereços MAC;
R.HS.C1.41	Implementar a pilha de protocolos TCP/IP na versão IPv4;
R.HS.C1.42	Permitir a atualização do relógio interno por meio de NTP (*Network Time Protocol*);
R.HS.C1.43	Implementar listas de controle de acesso (ACLs), baseados em endereços MAC, endereços IP, portas TCP e UDP;
R.HS.C1.44	Disponibilizar, no mínimo, dois níveis de senha de acesso, sendo uma com restrição total à configuração do equipamento e a comandos que alterem seu funcionamento, e outra sem qualquer restrição;
R.HS.C1.45	Implementar RADIUS e/ou TACACS+ ou similar;
R.HS.C1.46	Permitir a configuração de MAC autorizado em determinada porta assim como a quantidade máxima de MAC aprendido por porta;
R.HS.C1.47	Implementar funcionalidade que permita ao *switch* monitorar o tráfego DHCP e montar dinamicamente tabela que relacione os endereços MAC das estações com os respectivos endereços IP providos pelo servidor DHCP da rede, bloqueando pacotes DHCP em portas não autorizadas;
R.HS.C1.48	Permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados no equipamento;
R.HS.C1.49	Implementar IEEE 802.1ab *Link Layer Discovery Protocol* (LLDP);
R.HS.C1.50	Permitir o *download* e o *upload* das configurações de forma segura, por meio de SCP (*Secure Copy Protocol*) ou SFTP (*Secure File Transfer Protocol*);
R.HS.C1.51	Permitir a configuração através de *Secure Shell* (SSHv2) e porta de console;
R.HS.C1.52	Permitir a gravação de eventos por meio do protocolo *syslog*;
R.HS.C1.53	Possuir ferramentas de *debug* e *log* de eventos para depuração e gerenciamento em primeiro nível;
R.HS.C1.54	Implementar os padrões de gerência de rede SNMP-v2 e SNMP-v3 com autenticação e/ou criptografia, incluindo a geração de *traps*;
R.HS.C1.55	Possuir suporte a MIB II;
R.HS.C1.56	Possuir suporte nativo a dois grupos RMON (*Alarms* e *Events*), conforme RFC 1757, sem a utilização de *probes* externas;
R.HS.C1.57	Implementar *NetFlow* ou *SFlow* ou tecnologia similar sem a necessidade de *probes* externas;
R.HS.C1.58	Suportar múltiplas imagens de *firmware*;
R.HS.C1.59	Suportar o protocolo *Virtual Extensible* LAN (VXLAN) de acordo com a RFC 7348.

R.HS.C1.60	Deverá suportar automação através de ferramentas de desenvolvimento de *scripts* do tipo PYTHON ou JSON ou XML;
R.HS.C1.61	Possuir suporte à virtualização e *multipath* com base em VXLAN: • O equipamento deverá operar como gateway VXLAN permitindo a conectividade L2 entre uma VLAN e uma VXLAN; • O equipamento deverá implementar VXLAN *Bridging* permitindo a extensão de uma VLAN ou de uma VXLAN sobre uma nuvem IP (*Underlay*); • O equipamento deverá implementar VXLAN *Routing* permitindo a conectividade L3 entre VXLANs (de forma análoga à função de roteamento entre VLANs);
R.HS.C1.62	Suportar SDN/OpenFlow v1.3 ou superior;
R.HS.C1.63	Suportar automação de rede através de controladora centralizada podendo ser realizado por software ou hardware dedicado;
R.HS.C1.64	Implementar tunelamento de VLANs por meio de funcionalidade Q-in-Q;

Requisitos Tecnológicos (hardware e software) – *Switch Core Tipo 2*	
ID	**Descrição**
R.HS.C2.01	O equipamento deve ser novo e estar em linha de produção, ou seja, com suporte ativo e ciclo de vida garantido pelo fabricante por, no mínimo, 5 (cinco) anos;
R.HS.C2.02	O equipamento deve possuir, no mínimo, 40 portas 10GE SFP+ e, no mínimo, 4 portas 40GE QSFP+. As portas 40GE QSFP+ devem operar em modo *wirespeed* e *non-blocking*, compatíveis com: • *Transceivers padrões 40GBase-SR4 e 40GBase-LR4;* • Cabos QSFP+ *Direct Attach Cable* (DAC), conforme a especificação 40GBase-CR4. Não é permitida a utilização conversores externos;
R.HS.C2.03	Possuir uma porta de console com conector RJ-45 ou DB9 macho;
R.HS.C2.04	Possuir uma porta 10/100/1000 ou 1G/10G com conector RJ-45 para gerência *out-of-band* do equipamento;
R.HS.C2.05	Possuir na configuração ofertada fontes de alimentação redundantes e *hot-swappable*, onde a falha de uma fonte não deve implicar na parada de nenhuma função do equipamento;
R.HS.C2.06	As fontes de alimentação e a bandeja de ventiladores devem ser do tipo *hot-swappable*, devendo poder ser substituída sem que seja necessário desligar o equipamento, interromper seu funcionamento ou ter que retirar qualquer módulo;
R.HS.C2.07	Possuir capacidade de *switching* de, pelo menos, 2 Tbps;
R.HS.C2.08	Possuir taxa de encaminhamento de pacotes de no mínimo 1900 Mpps;
R.HS.C2.09	Implementar *switching* L2 e L3 localmente. O equipamento deve ser fornecido com todos os componentes necessários para esta finalidade;
R.HS.C2.10	Implementar roteamento estático com suporte a, no mínimo, 1000 (mil) rotas IPv4;
R.HS.C2.11	Implementar OSPF-v3 *full*, incluindo autenticação MD-5;
R.HS.C2.12	Implementar BGPv4;

R.HS.C2.13	Implementar roteamento IPv6;
R.HS.C2.14	Implementar agregação de *links* conforme padrão IEEE 802.3ad com, no mínimo, 24 grupos, permitindo até oito *links* agregados por grupo;
R.HS.C2.15	Implementar agregação de *links* conforme padrão IEEE 802.3ad com suporte a LACP;
R.HS.C2.16	Implementar agregação de *links* entre múltiplos *switches* (MLAG ou similar), possibilitando combinar a largura de banda de portas físicas pertencentes a *switches* físicos distintos;
R.HS.C2.17	Deve suportar o armazenamento de, no mínimo, 64.000 endereços MAC;
R.HS.C2.18	Implementar, no mínimo, 512 regras de ACL de saída (*egress ACLs*);
R.HS.C2.19	O equipamento deve implementar VRF (*Virtual Routing Forwarding*), MCE ou equivalente;
R.HS.C2.20	Implementar jumbo *frames* em todas as portas ofertadas, com suporte a pacotes de até 9000 *Bytes*;
R.HS.C2.21	Permitir a configuração de, no mínimo, 3965VLANs;
R.HS.C2.22	Implementar protocolo *Virtual Router Redundancy Protocol – VRRP-v2* e *VRRP-v3* ou mecanismo similar de redundância de *default gateway*;
R.HS.C2.23	Implementar STP (*Spanning Tree Protocol*) de acordo com o IEEE 802.1d, RSTP (*Rapid Reconfiguration for Spanning Tree Protocol*) de acordo IEEE 802.1w e 802.1D e MSTP (*Multiple Instances of Spanning Tree Protocol*) de acordo com IEEE 802.1s;
R.HS.C2.24	Implementar PVST+ ou similar;
R.HS.C2.25	Implementar VLAN (*Virtual bridged Local Area Network*) e VLANs *Tagging* de acordo com IEEE 802.1Q;
R.HS.C2.26	Suportar autenticação baseada em MAC ou WEB;
R.HS.C2.27	Implementar QoS de acordo com IEEE 802.1p;
R.HS.C2.28	Implementar os algoritmos de gerenciamento de filas WRR (*Weighted Round Robin*) ou DWRR (*Deficit Weighted Round Robin*) ou WFW (*Weighted Fair Queuing*) e SP (*Strict Priority*) ou WRED (*Weighted Random Early Detection*) e SP (*Strict Priority*);
R.HS.C2.29	Suportar IGMPv2 ou superior e IGMP *Snooping* para controle de tráfego *multicast*;
R.HS.C2.30	Permitir a suspensão de recebimento de BPDUs (*Bridge Protocol Data Units*) caso a porta esteja colocada no modo *fast forwarding*, conforme previsto no padrão IEEE 802.1w. Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
R.HS.C2.31	Permitir o espelhamento do tráfego de entrada e saída de múltiplas portas do *switch* em uma única porta;
R.HS.C2.32	Implementar DHCP-*Relay* permitindo a definição de pelo menos 2 servidores DHCP;
R.HS.C2.33	Implementar DHCP *snooping* ou funcionalidade similar que permita o bloqueio de servidores DHCP não autorizados na rede;
R.HS.C2.34	Permitir a classificação e priorização de pacotes baseada em informações de camada 2, 3 e 4 do modelo OSI, para no mínimo: Endereço MAC, endereço IP, número de porta TCP ou UDP, valor do campo CoS (802.1p) e valor do campo ToS (com precedência IP e DSCP);
R.HS.C2.35	Permitir a configuração de, no mínimo, oito filas de prioridade por porta;

R.HS.C2.36	Permitir a limitação de endereços MAC por porta. Os endereços MAC podem ser aprendidos automaticamente ou configurados manualmente;
R.HS.C2.37	Possuir mecanismos para controle dos tráfegos de *broadcast*, *multicast* e *unknown-unicast* (ou funcionalidade similar para o controle de tráfego *unknown-unicast*) por porta. Deve ser possível especificar limites individuais para tráfego tolerável de *broadcast*, *multicast* e *unknown-unicast* em cada porta do *switch*;
R.HS.C2.38	Permitir a limitação de tráfego (*rate limiting*);
R.HS.C2.39	Implementar roteamento entre as VLANs internamente, sem a necessidade de equipamentos externos;
R.HS.C2.40	Implementar filtros baseados em protocolos e endereços MAC;
R.HS.C2.41	Implementar a pilha de protocolos TCP/IP na versão IPv4;
R.HS.C2.42	Permitir a atualização do relógio interno por meio de NTP (*Network Time Protocol*);
R.HS.C2.43	Implementar listas de controle de acesso (ACLs), baseados em endereços MAC, endereços IP, portas TCP e UDP;
R.HS.C2.44	Disponibilizar, no mínimo, dois níveis de senha de acesso, sendo uma com restrição total à configuração do equipamento e a comandos que alterem seu funcionamento, e outra sem qualquer restrição;
R.HS.C2.45	Implementar RADIUS e/ou TACACS+ ou similar;
R.HS.C2.46	Permitir a configuração de MAC autorizado em determinada porta assim como a quantidade máxima de MAC aprendido por porta;
R.HS.C2.47	Implementar funcionalidade que permita ao *switch* monitorar o tráfego DHCP e montar dinamicamente tabela que relacione os endereços MAC das estações com os respectivos endereços IP providos pelo servidor DHCP da rede, bloqueando pacotes DHCP em portas não autorizadas;
R.HS.C2.48	Permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados no equipamento;
R.HS.C2.49	Implementar IEEE 802.1ab *Link Layer Discovery Protocol* (LLDP);
R.HS.C2.50	Permitir o *download* e o *upload* das configurações de forma segura, por meio de SCP (*Secure Copy Protocol*) ou SFTP (*Secure File Transfer Protocol*);
R.HS.C2.51	Permitir a configuração através de *Secure Shell* (SSHv2) e porta de console;
R.HS.C2.52	Permitir a gravação de eventos por meio do protocolo *syslog*;
R.HS.C2.53	Possuir ferramentas de *debug* e *log* de eventos para depuração e gerenciamento em primeiro nível;
R.HS.C2.54	Implementar os padrões de gerência de rede SNMP-v2 e SNMP-v3 com autenticação e/ou criptografia, incluindo a geração de *traps*;
R.HS.C2.55	Possuir suporte a MIB II;
R.HS.C2.56	Possuir suporte nativo a dois grupos RMON (*Alarms* e *Events*), conforme RFC 1757, sem a utilização de *probes* externas;
R.HS.C2.57	Implementar *NetFlow* ou *SFlow* ou tecnologia similar sem a necessidade de *probes* externas;
R.HS.C2.58	Suportar múltiplas imagens de *firmware*;
R.HS.C1.59	Suportar o protocolo *Virtual Extensible* LAN (VXLAN) de acordo com a RFC 7348.
R.HS.C1.60	Deverá suportar automação através de ferramentas de desenvolvimento de *scripts* do tipo PYTHON ou JSON ou XML;

R.HS.C1.61	Possuir suporte à virtualização e *multipath* com base em VXLAN: • O equipamento deverá operar como gateway VXLAN permitindo a conectividade L2 entre uma VLAN e uma VXLAN; • O equipamento deverá implementar VXLAN *Bridging* permitindo a extensão de uma VLAN ou de uma VXLAN sobre uma nuvem IP (*Underlay*); • O equipamento deverá implementar VXLAN *Routing* permitindo a conectividade L3 entre VXLANs (de forma análoga à função de roteamento entre VLANs);
R.HS.C1.62	Suportar SDN/OpenFlow v1.3 ou superior;
R.HS.C1.63	Suportar automação de rede através de controladora centralizada podendo ser realizado por *software* ou *hardware* dedicado;
R.HS.C1.64	Implementar tunelamento de VLANs por meio de funcionalidade Q-in-Q;

Requisitos Tecnológicos (hardware e software) – *Switch* ACESSO	
ID	**Descrição**
R.HS.A01	Para fins de compatibilidade, deve ser do mesmo fabricante dos demais equipamentos descritos neste termo;
R.HS.A02	A solução deve ser composta de um único equipamento, devendo este vir acompanhado dos devidos acessórios para tal, inclusive do cabo de alimentação;
R.HS.A03	Os *switches* tipo 1 deverão possuir altura máxima de 1U (1,75’’); os *switches* tipo 2 e 3 deverão, além de possuir altura máxima de 1U (1,75’’), ser montável em rack 19’’;
R.HS.A04	O equipamento deve ser novo e estar em linha de produção, ou seja, com suporte ativo e ciclo de vida garantido pelo fabricante por, no mínimo, 5 anos;
R.HS.A05	Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60Hz, com detecção automática de tensão e frequência;
R.HS.A06	Deve possuir arquitetura que utilize memória não volátil para armazenamento do sistema operacional e das configurações;
R.HS.A07	Ser fornecido com configuração de CPU e memória (RAM e *Flash*) suficiente para implementação de todas as funcionalidades descritas nesta especificação, simultaneamente;
R.HS.A08	A memória *flash* instalada deve ser suficiente para comportar, no mínimo, duas imagens do sistema operacional simultaneamente, permitindo que seja feito um *upgrade* de *software* e a imagem anterior seja mantida;
R.HS.A09	Possuir capacidade de encaminhamento de pacotes de, no mínimo: • 40 Mpps para *switches* de acesso tipo 1; • 93 Mpps para *switches* de acesso tipo 2; • 112 Mpps para *switches* de acesso tipo 3;
R.HS.A10	Possuir capacidade de *switching* de pelo menos: • 55 Gbps para *switches* de acesso tipo 1; • 128 Gbps para *switches* de acesso tipo 2; • 176 Gbps para *switches* de acesso tipo 3;
R.HS.A11	Implementar detecção automática MDI/MDIX em todas as portas UTP RJ-45;
R.HS.A12	Possuir por de console com conector RJ-45 ou DB9 macho;
R.HS.A13	Possuir *leds* indicativos de funcionamento da fonte de alimentação e status das

	portas;
R.HS.A14	Implementar auto-*negotiation* e *auto*-sensing de forma automática em todas as portas do *switch*, no modo *full duplex*;
R.HS.A15	Implementar o protocolo IEEE 802.3at *Power over Ethernet* (*PoE*), provendo, no mínimo, por porta: • *Switch* de acesso tipo 1: 15.4w. Com, no mínimo, 120w de potência; • *Switch* de acesso tipo 2: 15.4w. Com, no mínimo, 370w de potência; • *Switch* de acesso tipo 3: 15.4w. Com, no mínimo, 740w de potência; Caso seja necessário qualquer item adicional para garantir essa funcionalidade, o mesmo deverá ser entregue e instalado, sem ônus para a contratante;
R.HS.A16	Os *switches* de acesso deverão possuir: • Tipo 1 – 8 (oito) portas 100/1000GbE-BaseT; • Tipo 2 – 24 (vinte e quatro) portas 10/100/1000GbE-BaseT; • Tipo 1 – 48 (quarenta e oito) portas 10/100/1000GbE-BaseT;
R.HS.A17	Os *switches* tipo 1 deverão possuir, no mínimo, 2 portas 10GBASE-X SFP+, *non-blocking*, ativas simultaneamente, devendo um mesmo *slot* suportar interfaces 10 GBase-SR e 10GBase-LR. Não é permitida a utilização conversores externos;
R.HS.A18	Todas as interfaces *Gigabit Ethernet* devem funcionar simultaneamente;
R.HS.A19	Para os *switches* de acesso tipo 2 e tipo 3, implementar empilhamento de, no mínimo, 4 equipamentos e gerência através de um único endereço IP;
R.HS.A20	Para os *switches* de acesso tipo 2 e tipo 3, o equipamento deve possuir, no mínimo, 2 portas para empilhamento com velocidade de pelo menos 20 Gbps cada (ou 10 Gbps *Full Duplex*) , *non-blocking*, ou tecnologia similar com desempenho igual ou superior ao empilhamento supracitado;
R.HS.A21	Para os *switches* de acesso tipo 2 e tipo 3, o equipamento deve permitir a operação simultânea de, no mínimo, 2 portas de empilhamento e 2 portas de *uplink* 10 Gbps *Ethernet* SFP+ *Full Duplex*, cada, sem prejudicar o funcionamento das demais portas *Gigabit Ethernet*;
R.HS.A22	Para os *switches* de acesso tipo 2 e tipo 3, deverão ser utilizadas interfaces DAC, com no mínimo, 0,5 metros, para empilhamento dos *switches*. Caso o equipamento ofertado não possua o recurso descrito no requisito RHS.A21, a Contratada deverá fornecer todo e qualquer elemento necessário para o correto empilhamento e *uplink* dos *switches*, tais como cabos, módulos, *etc*. Ou seja, cada *switch* de acesso tipo 2 e tipo 3 deverá possuir uma porta dedicada para empilhamento e um cabo com, no mínimo, 0,5 metros.
R.HS.A23	O empilhamento deve ter capacidade de *path fast recover*, ou seja, com a falha de um dos elementos da pilha os fluxos devem ser reestabelecidos no tempo máximo de 2 segundos;
R.HS.A24	O empilhamento deve permitir, conforme padrão 802.3AD, a criação de, no mínimo, 6 grupos, permitindo até: • *Switch* de acesso tipo 2: 4 *links* agregados entre diferentes membros da pilha; • *Switch* de acesso tipo 3: 8 *links* agregados entre diferentes membros da pilha;
R.HS.A25	O empilhamento deve suportar espelhamento de tráfego entre diferentes

	unidades da pilha;
R.HS.A26	O empilhamento deverá suportar arquitetura de anel para prover resiliência;
R.HS.A27	Implementar agregação de *links* conforme padrão IEEE 802.3AD com suporte a LACP;
R.HS.A28	Suportar o armazenamento de, no mínimo, 16.000 (dezesseis mil) endereços MAC;
R.HS.A29	Permitir a limitação de endereços MAC por porta. Os endereços MAC podem ser aprendidos automaticamente ou configurados manualmente. No caso da quantidade de endereço MAC ser excedida, deverá ser possível configurar ações de descarte por pacotes não autorizados e desabilitar definitivamente a porta;
R.HS.A30	Implementar *jumbo frames* em todas as portas ofertadas, com suporte a pacotes de até 9000 *Bytes*;
R.HS.A31	Implementar *Private Vlans* ou similar;
R.HS.A32	Implementar STP (*Spanning Tree Protocol*) de acordo com o IEEE 802.1d, RSTP (*Rapid Reconfiguration for Spanning Tree Protocol*) de acordo IEEE 802.1w e 802.1D e MSTP (*Multiple Instances of Spanning Tree Protocol*) de acordo com IEEE 802.1s;
R.HS.A33	Implementar VLAN (*Virtual bridged Local Area Network*) e VLANs *Tagging* de acordo com IEEE 802.1Q, permitindo a configuração de, no mínimo, 4090 *VLANs*;
R.HS.A34	Implementar roteamento entre as VLANs internamente sem a necessidade de equipamentos externos;
R.HS.A35	Implementar *Port-Based Network Access Control for Network Login*, de acordo com IEEE 802.1x;
R.HS.A36	Suportar autenticação baseada em endereço MAC, inclusive por servidor RADIUS;
R.HS.A37	Suportar *Guest VLAN* de acordo com IEEE 802.1p;
R.HS.A38	Implementar QoS de acordo com IEEE 802.1p, incluindo a leitura, classificação e remarcação de QoS (802.1p e DSCP);
R.HS.A39	Implementar remarcação de prioridade de pacotes *Layer 3*, remarcando o campo *DiffServ* para grupos de tráfego classificados segundo portas TCP e UDP, endereço/sub-rede IP e MAC origem e destino;
R.HS.A40	Implementar quatro filas de prioridade em *hardware* por porta;
R.HS.A41	Permitir a classificação e priorização de pacotes baseada em informações de camada 2, 3 e 4 do modelo OSI, para no mínimo endereço MAC, endereço IP, número de porta TCP ou UDP, valor do campo CoS (802.1p) e valor do campo ToS (com precedência IP e DSCP);
R.HS.A42	Suportar IGMP v2 ou superior e IGMP *Snooping* para controle de tráfego *multicast*;
R.HS.A43	Permitir a suspensão de recebimento de BPDUs (*Bridge Protocol Data Units*) caso a porta esteja colocada no modo *fast forwarding*, conforme previsto no padrão IEEE 802.1w. Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
R.HS.A44	Permitir o espelhamento do tráfego de entrada e saída de múltiplas portas do *switch* em uma única porta;
R.HS.A45	Implementar DHCP Server permitindo a distribuição de endereços e parâmetros

	nativos a este tipo de serviço;
R.HS.A46	Implementar DHCP *Relay* permitindo a definição de pelo menos dois servidores DHCP;
R.HS.A47	Implementar funcionalidade que permita que somente endereços designados por um servidor DHCP tenham acesso à rede;
R.HS.A48	Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (*Trusted DHCP Server*);
R.HS.A49	Possuir mecanismos para controle dos tráfegos de *broadcast*, *multicast* e *unknown-unicast* (ou funcionalidade similar para o controle de tráfego *unknown-unicast*) por porta. Deve ser possível especificar limites individuais para tráfego tolerável de *broadcast*, *multicast* e *unknown-unicast* em cada porta do *switch*;
R.HS.A50	Permitir limitação de tráfego (*rate limiting*);
R.HS.A51	Implementar filtros baseados em protocolos e endereços MAC;
R.HS.A52	Implementar a pilha de protocolos TCP/IP na versão IPv4;
R.HS.A53	Permitir a atualização do relógio interno por meio de NTP ou SNTP;
R.HS.A54	Implementar listas de controle de acesso (ACLs) baseadas em endereços MAC, endereços IP, portas TCP e UDP;
R.HS.A55	Disponibilizar, no mínimo, dois níveis de senha de acesso, sendo uma com restrição total à configuração do equipamento e a comandos que alterem seu funcionamento, e outra sem qualquer restrição;
R.HS.A56	Implementar controle de acesso por porta segundo o padrão IEEE 802.1x, com configuração dinâmica da VLAN do usuário autenticado;
R.HS.A57	Implementar autenticação de usuário através do padrão 802.1x associando automaticamente o usuário à VLAN, segundo parâmetros fornecidos na etapa de *login*;
R.HS.A58	Implementar RADIUS e/ou TACACS+ ou similar, segundo a RFC1492;
R.HS.A59	Implementar funcionalidade que permita ao *switch* monitorar o tráfego DHCP e montar dinamicamente tabela que relacione os endereços MAC das estações com os respectivos endereços IP providos pelo servidor DHCP da rede, bloqueando pacotes DHCP em portas não autorizadas ou funcionalidade similar de DHCP *Snooping*;
R.HS.A60	Permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados no equipamento;
R.HS.A61	Implementar IEEE 802.1ab *Link Layer Discovery Protocol LLDP*;
R.HS.A62	Implementar gerenciamento via *web* com suporte a HTTP e HTTPS;
R.HS.A63	Permitir o *download* e o *upload* das configurações, de forma segura, por meio de SCP (*Secure Copy Protocol*) ou SFTP (*Secure File Transfer Protocol*);
R.HS.A64	Permitir a configuração através de *Secure Shell* (SSH v2) e porta de console;
R.HS.A65	Permitir a gravação de eventos por meio do protocolo *syslog*;
R.HS.A66	Possuir ferramentas de *debug* e *log* de eventos para depuração e gerenciamento em primeiro nível;
R.HS.A67	Implementar os padrões de gerência de rede SNMP v2 e SNMP v3 com autenticação e/ou criptografia, incluindo a geração de *traps*;
R.HS.A68	Possuir suporte a MIB II;
R.HS.A69	Possuir suporte nativo a quatro grupos RMON (*History*, *Statistics*, *Alarms* e

	Events) conforme RFC 1757, sem a utilização de *probes* externas;
R.HS.A70	Deve implementar mecanismo interno para responder a pacotes de teste de desempenho de rede, com capacidade de medir latência de conexões TCP e *jitter* de conexões UDP;
R.HS.A71	Devem ser suportadas, no mínimo, as seguintes opções de teste a partir do *switch* ofertado: • ICMP *echo*; • TCP *connect* (em qualquer porta TCP do intervalo 1-65535 que o administrador especifique); • UDP *echo* (em qualquer porta UDP do intervalo 1-65535 que o administrador especifique);
R.HS.A72	Deve implementar, em *hardware*, tecnologia para monitoramento de tráfego que permita agrupar os pacotes que circulam pelo equipamento usando o conceito de fluxos (*flows*).
R.HS.A73	De forma a garantir alta visibilidade do tráfego de rede, para cada fluxo devem ser exibidas, no mínimo, as seguintes informações; • Endereços IP de origem/destino; • Portas TCP/UDP de origem/destino; • Interfaces de entrada e saída do tráfego; • Número de pacotes transmitidos.
R.HS.A74	As informações coletadas devem ser automaticamente exportáveis em intervalos pré-definidos através de *NetFlow v9* ou conforme a RFC 7011. A ativação dessa funcionalidade não poderá alterar o desempenho do *switch*;
R.HS.A75	Deverá possuir memória de *buffer* de, no mínimo 10MB para tratamento de tráfego;
R.HS.A76	Deverá possuir automação de operação, monitoramento e resolução de problemas através de linguagem de programação, suportando, no mínimo, linguagens REST e *Openflow*;
R.HS.A77	Deverá possuir mecanismo para monitorar a qualidade do tráfego de voz e realizar testes de VoIP através de UDP *Jitter*;
R.HS.A78	Deverá possuir mecanismo para monitorar os parâmetros e configurações dos *transceivers*;
R.HS.A79	Possibilitar o seu gerenciamento através do Sistema de Gerenciamento da solução;

Requisitos Tecnológicos (*Software* de Gerência e Controle de Acesso) – Console de Gerenciamento	
ID	**Descrição**
R.SG.CG01	A solução é composta pelo Sistema de Gerenciamento Centralizado e Sistema de Controle de Acesso;
R.SG.CG02	A solução deverá ser fornecida na forma de *Appliance* Virtual ou *software* sendo executado em sistemas operacionais x86-x64;
R.SG.CG03	Caso a solução ofertada seja em forma de *Appliance Virtual*, a solução deve ser fornecida já instalada e preparada, em uma plataforma *VMware vSphere* 6; • A instalação da solução deverá utilizar a infraestrutura de virtualização da Contratante; • Não haverá necessidade do fornecimento de qualquer licença de

	produtos da *VMware*. Toda a estrutura de virtualização será provida pela infraestrutura tecnológica do Contratante;
R.SG.CG04	Caso a solução ofertada seja baseada em *software* executados em sistemas operacionais x86-x64, será permitido o uso de sistema operacional e SGBD da infraestrutura tecnológica do Contratante, sem a necessidade de licenças adicionais. Sendo que: • O TST dispõe de licenças de sistemas operacionais *Microsoft Windows Server 2012R2* e *Oracle Linux 6* ou *Oracle Linux 7*; • O TST dispõe de licenças de sistemas de gerenciamento de banco de dados *Oracle* 12c e *Microsoft SQL Server 2008 R2*; • Não serão aceitas soluções que utilizem servidores de banco de dados com SGBD comerciais diferentes daqueles já instalados no TST, exceto o previsto no item R.SG.CG05;
R.SG.CG05	Serão admitidas soluções que possuam banco de dados proprietário, desde que estejam instalados em *Appliances* Virtuais;
R.SG.CG06	Todos os componentes da solução devem ser homologados pelo Fabricante, e suportado pela Contratada de maneira a garantir a padronização e interoperabilidade entre todos os componentes;
R.SG.CG07	Todos os componentes da solução, programas e sistemas operacionais devem estar em linha de produção do Fabricante. Não deve haver previsão de descontinuidade de comercialização e/ou suporte (*end-of-life* e *end-of-support*);
R.SG.CG08	Caso os componentes da solução, programas, sistemas operacionais e *appliances* virtuais recebam atualizações tecnológicas por parte do Fabricante, as mesmas deverão ser disponibilizadas ao Contratante sem qualquer ônus adicional durante toda a vigência do Contrato, mesmo que mudem de nome ou de *part number*;
R.SG.CG09	Não serão aceitos sistemas baseados em *software* de código aberto de uso genérico ou sistemas baseados em *software* sistema operacional diferentes daqueles oferecidos pelo fabricante para o mercado em geral;
R.SG.CG10	Os *softwares* deverão ser homologados pelo Fabricante, o que deverá ser comprovado através de documentação;
R.SG.CG11	Todos os componentes que farão parte da estrutura da solução deverão suportar redundância em conjunto de, no mínimo, dois componentes;
R.SG.CG12	No caso de falha de um dos componentes do conjunto, o outro deve ser capaz de assumir todas as operações e funcionalidade sem interrupção dos serviços;
R.SG.CG13	Deverá ser administrável remotamente por meio de interface gráfica (GUI) e/ou console de gerenciamento desde que este último seja compatível com *Microsoft Windows 10* (versão 64 *bits*), utilizando canais autenticados e criptografados;
R.SG.CG14	Deverá conter mecanismo de comunicação em tempo determinado pelo administrador entre o cliente e o servidor para consulta de novas configurações e políticas;
R.SG.CG15	Deve ser capaz de admitir integração com *Microsoft Active Direct* para um único *login* do usuário (*single sign on*);
R.SG.CG16	Deve ter a possibilidade de aplicar regras diferenciadas baseando em diferentes topologias e/ou segmentação lógica da rede;

R.SG.CG17	Deve ter a possibilidade de aplicar regras diferenciadas por grupos de usuários e máquinas;
R.SG.CG18	Possuir recursos para a criação e agendamento periódicos de *backups* da base de dados;
R.SG.CG19	Possuir capacidade de criação de contas de usuário com, pelo menos três diferentes níveis de acesso: administração, auditoria e operação;
R.SG.CG20	As atualizações das configurações dos ativos de rede deverão ser realizadas sem a utilização de *login scripts*, agendamento ou tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução;
R.SG.CG21	Todos os registros de *logs* da solução devem ser compatíveis com o padrão *syslog* conforme RFC-5424 e RFC-5426;
R.SG.CG22	Utilizar os protocolos HTTPS e SSH para comunicação com a console de gerenciamento;
R.SG.CG23	Autenticar, Autorizar e Auditar (AAA) usuários administrativos por meio do protocolo TACACS+;
R.SG.CG24	A solução deverá permitir escalabilidade horizontal, ou seja, suportar a inclusão de novos dispositivos com a simples adição de novos *appliances* na infraestrutura do TST, sem impacto na disponibilidade da solução;
R.SG.CG25	Possuir recursos nativos para a replicação do banco de dados entre os servidores de gerenciamento;
R.SG.CG26	A solução deve permitir conectividade para o(s) servidor(es) de gerência pré-definido(s), mesmo em uma política completamente restritiva. Isso permite que o cliente continue enviando relatórios e recebendo atualizações de políticas e remediações em arquitetura que utilizem agentes;
R.SG.CG27	Em caso de contingência operacional (caso algum dos componentes centrais da Solução venha a falhar), a parte restante do *cluster* deverá assumir automaticamente (sem intervenção humana) o processamento do(s) componente(s) afetado(s) em 100% sem ultrapassar 90% de sua capacidade de processamento total;
R.SG.CG28	Trabalhar em modo *cluster* de alta disponibilidade, com pelo menos dois nós ativo/ativo, podendo os nós estar localizados em locais geográficos distintos e em sub-redes distintas;
R.SG.CG29	Todos os componentes da solução deverão funcionar de forma independente de qualquer vínculo e/ou conexão com o fornecedor e/ou fabricante;
R.SG.CG30	Permitir o gerenciamento e configuração centralizada das políticas da Solução;
R.SG.CG31	Suportar o sincronismo de tempo via NTP (*Network Time Protocol*);
R.SG.CG32	Suportar execução manual e/ou programada de *backup*;

Requisitos Tecnológicos (*Software* de Gerência e Controle de Acesso) – Gerenciamento de Ativos de Rede	
ID	**Descrição**
R.SG.GAR01	Ter conformidade com a RFC 3580 (IEEE 802.1x), RFC 3416 (SNMP v2c) e RFC 3410 (SMNP v3) e RFC 3576/5176 (*Change of Authorization - CoA*);
R.SG.GAR02	Alterar configurações nos *switches* de forma remota e centralizada;
R.SG.GAR03	Realizar mudança da VLAN e ACL de acordo com a política definida, com ou sem o uso de 802.1x;
R.SG.GAR04	Receber eventos SNMP: recebimento de *traps* e via leitura de MIBs em TCP

	e/ou UDP;
R.SG.GAR05	Efetuar a instalação, configuração e atualização com *patches* do fabricante de todos os componentes da Solução, incluindo *software* e *appliances*;
R.SG.GAR06	Possuir usuário distinto com acesso irrestrito sobre a Solução;
R.SG.GAR07	Suportar a autorização centralizada via endereço MAC como opção de acesso para elementos de rede sem suplicante 802.1x ("*MAC authentication bypass*");
R.SG.GAR08	Permitir *login* integrado (*single sign on*) com a base de usuários *Microsoft Active Directory*;

Requisitos Tecnológicos (*Software* de Gerência e Controle de Acesso) – Acesso à Rede	
ID	**Descrição**
R.SG.AR01	A solução deve integrar de forma transparente com dispositivos de segurança, *switches* e roteadores, no mínimo, dos seguintes fabricantes: • *Cisco*; • *Dell*; • *Extreme*; • HPE.
R.SG.AR02	Possibilidade de bloquear a comunicação ponto a ponto entre máquinas que estiverem em conformidade com as políticas de controle de acesso à rede e máquinas que não estiverem em conformidade com as políticas de controle de acesso à rede;
R.SG.AR03	Suportar protocolo EAP e PEAP;
R.SG.AR04	A Solução deverá tomar ações como ativar ou desativar a porta do *switch* e/ou trocar de VLAN;
R.SG.AR05	Caso a Solução necessite de agente, deve ser possível o fornecimento de agentes, via *web*, para máquinas não gerenciadas;
R.SG.AR06	A Solução deve ter capacidade de *profiling* para descoberta de dispositivos conectados à rede;
R.SG.AR07	A Solução deverá permitir aplicação de regras baseadas em grupos do *Active Directory*;

Requisitos Tecnológicos (*Software* de Gerência e Controle de Acesso) – Relatórios e Monitoramento	
ID	**Descrição**
R.SG.RM01	A Solução deverá fornecer alerta na console de gerência via SMTP e SMS;
R.SG.RM02	A Solução deverá possibilitar aos administradores do sistema a geração de relatórios customizados exportáveis nos formatos PDF, CSV e TXT;
R.SG.RM03	A Solução deverá fornecer as seguintes informações de gráfica, incluindo: • Tipos de dispositivos; • Fabricante do dispositivo; • Sistema Operacional; • Endereço IP associado; • Informações do usuário; • Conexões; • Políticas em uso; • Regras de Controle de Acesso.

R.SG.RM04	A Solução deverá gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos os seus componentes. Os registros de *logs* devem conter a identificação do evento, data e hora, identificação do usuário, identificação do dispositivo e endereço IP do dispositivo;
R.SG.RM05	A Solução deverá gerar e armazenar registros de *logs* com informações sobre falhas e erros ocorridos na console de gerenciamento, nos dispositivos e nos portais de autosserviço;
R.SG.RM06	Centralizar *logs* de diversos *appliances* em um único ponto central;
R.SG.RM07	Possuir ferramentas para acompanhamento e análise de eventos e estatística de *logs*;
R.SG.RM08	Os acessos à administração e configuração, bem como as alterações realizadas durante o acesso, devem ser registrados em *log*, informando no mínimo a data, hora, IP de origem e usuário;

Requisitos Tecnológicos (*Software* de Gerência e Controle de Acesso) – Solução de AAA	
ID	**Descrição**
R.SG.AAA01	Executar a função de servidor de arquitetura AAA (*Authentication, Authorization and Accounting*) autenticando os ativos através dos protocolos TACACS+ e RADIUS;
R.SG.AAA02	Autorizar, através dos protocolos TACACS+ ou RADIUS, a execução de comandos para usuários de serviço e usuário administradores;
R.SG.AAA03	Controlar o acesso administrativo a equipamentos de rede IPv4;
R.SG.AAA04	A Solução deverá garantir redundância e operar em alta disponibilidade e suportar a recuperação de indisponibilidade de forma automática em todas as partes da Solução, sem perda das informações e configurações de AAA;
R.SG.AAA05	A adição de novos componentes não pode interferir nos serviços de AAA providos pela Solução;
R.SG.AAA06	Replicar sua base de dados, com perfis de acesso, grupos de ativos e suas configurações de AAA entre os nós do cluster;
R.SG.AAA07	Possuir acesso controlado e autenticado por usuário;
R.SG.AAA08	Permitir a definição local da base de usuários/senhas para usuários administradores;
R.SG.AAA09	Permitir a definição de grupos de usuários internos para a administração da Solução;
R.SG.AAA10	Fornecer perfis de acesso de suporte, manutenção, segurança e monitoração da própria Solução;
R.SG.AAA11	Permitir a configuração de políticas de senha para os usuários;
R.SG.AAA12	Permitir, de forma centralizada, a criação de grupos de ativos de rede;
R.SG.AAA13	Permitir, de forma centralizada, a criação de grupos de usuários;
R.SG.AAA14	Permitir, de forma centralizada, a criação de grupos de comandos e/ou perfis de acesso para os usuários administradores;
R.SG.AAA15	Possuir interface gráfica de administração com telas que apresentem de forma detalhada as informações relativas às últimas 24 (vinte e quatro) horas de operação contendo, no mínimo, o número de dispositivos ativos, sucesso e falhas de autenticação. Todas essas informações devem ser acompanhadas do horário da ocorrência;
R.SG.AAA16	Permitir associar um ou mais grupos de usuários a um ou mais grupos de

	ativos;
R.SG.AAA17	Permitir a alteração da quantidade de grupos de equipamentos, seus nomes e suas associações com grupos de usuários e perfis de acesso a qualquer momento;
R.SG.AAA18	Suportar, pelo menos, as seguintes famílias de atributos RADIUS: • Atributos definidos pelo IETF; • Atributos *Microsoft*; • Atributos *Cisco* RADIUS.
R.SG.AAA19	Suportar a exportação de *logs* de AAA no formato TXT;
R.SG.AAA20	Registrar no servidor da Solução os *logs* de AAA, com estampa de tempo (*timestamp*) de todos os comandos executados por usuários autorizados e todas as tentativas não autorizadas de execução de comandos. Gerar relatórios pré-definidos de utilização dos serviços de controle de acesso provendo as seguintes informações: • Usuários autenticados com sucesso; • Comandos executados pelo usuário com sucesso; • Comandos negados e o motivo da negação; • Falhas de autenticação e motivo das falhas; • RADIUS *accounting*; • Relatórios de administração dos *appliances*; • Relatórios TOP N; • Deve ser possível criar relatórios personalizados.
R.SG.AAA21	Permitir o expurgo de *logs* de AAA de forma manual, automática e customizado por período;
R.SG.AAA22	Permitir a autenticação de conexões EAP para uso em ambientes com IEEE 802.1x. A solução deve ter a capacidade de registrar, no mínimo, os seguintes parâmetros de acesso: • Usuário e grupo a qual este pertence; • *Switch* através do qual o acesso foi solicitado; • Porta do *switch* na qual o usuário estava conectado; • Endereço MAC da máquina usada pelo usuário; • *Bytes* transmitidos e recebidos durante o período de conexão.
R.SG.AAA23	A Solução deve suportar pelo menos os seguintes métodos: • EAP; • EAP-md5; • EAP-TLS; • PEAP; • EAP-*fast*.
R.SG.AAA24	A Solução deve suportar uso simultâneo de usuários;
R.SG.AAA25	Utilizar o protocolo TCP para prover maior confiabilidade ao tráfego dos pacotes envolvidos no controle administrativo (Servidor TACACS+);
R.SG.AAA26	Implementar os mecanismos de AAA com garantia de entrega, criptografando todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
R.SG.AAA27	Possuir filtro de acesso via IP de origem para a interface *WEB* da Solução.

Requisitos do Serviço de Instalação – *Switch Core Tipo 1, 2*	
ID	**Descrição**
R.SI.C01	A Contratada deverá realizar a instalação, configuração e operação dos equipamentos fornecidos na cidade sede da Contratante;
R.SI.C02	Caberá à Contratada incluir a apresentação do projeto conceitual, cronograma e fases de execução;
R.SI.C03	Caberá à Contratada a instalação lógica dos comutadores incluindo todos os componentes necessários para o perfeito funcionamento da solução integrada com o parque computacional já existente;
R.SI.C04	Caberá à Contratada incluir o levantamento das conexões e configurações do equipamento a ser substituído;
R.SI.C05	Contemplar a execução da instalação/migração/configuração, além da otimização e testes de validação;
R.SI.C06	Caberá à Contratada incluir a transferência de conhecimento de todos os procedimentos executados durante e após a migração para a equipe técnica do TST, constatando de apresentação técnica detalhada com diagramas gráficos e comandos executados;
R.SI.C07	Caberá à Contratada incluir a entrega da documentação completa da nova solução, contemplando diagramas físicos e lógicos, planilhas detalhadas com as faixas de rede configurada em cada porta do equipamento, *As-Build* completo, planilha com *part numbers*, etc.

Requisitos do Serviço de Instalação – *Switch* Acesso	
ID	**Descrição**
R.SI.A01	Caberá à Contratada todo o processo de planejamento, configuração, integração, testes e compatibilidade, que deverão ser integrados à infraestrutura de Tecnologia da Informação existente no TST;
R.SI.A02	A equipe técnica da CITEC disponibilizará um ambiente para que a Contratada possa definir o modelo base de configuração dos *switches* de acesso;
R.SI.A03	Após a aprovação deste modelo a equipe técnica do TST assumirá a instalação e configuração de todos os *switches* de acesso;

Requisitos de Treinamento (Capacitação)	
ID	**Descrição**
R.T01	A Contratada deverá fornecer treinamento oficial, podendo ocorrer nas dependências do TST ou em local próprio indicado pela Contratada;
R.T02	Todos os custos envolvidos com o treinamento deverão ser de responsabilidade da Contratada, incluindo hospedagem e passagem, caso não seja realizado em Brasília;
R.T03	O treinamento deverá ser focado na aprendizagem e no desenvolvimento de habilidades práticas necessárias para configurar e gerenciar o ambiente;
R.T04	O conteúdo deverá abordar, no mínimo, os seguintes tópicos: • Visão geral dos equipamentos adquiridos (resumo de comandos CLI); • *Interfaces* (Física, *Link Aggregation* ou equivalente, VLAN); • *Spanning-tree*; • *Fabric* (Introdução, Arquiteturas, Implementação, Gerenciamento e

	Troubleshooting); • ACLs (Introdução, Configuração e Utilização de *Access Control List*); • VRRP ou equivalente (Introdução, Configuração e *Troubleshooting*); • OSPF v3 (Introdução, Configuração e *Troubleshooting*); • *Multi-Chassis Link Aggregation* ou equivalente (Introdução, Configuração, Gerenciamento e *Troubleshooting*); • *Stacking* (Introdução, Configuração, Gerenciamento e *Troubleshooting*); • Solução de Gerenciamento (Introdução, Implementação e Utilização avançada);
R.T05	O treinamento deverá ter carga horária de pelo menos 24 (vinte e quatro) horas, durante 4 (quatro) dias, sendo 6 (seis) horas ao dia;
R.T06	Os cursos deverão habilitar o participante a gerenciar a solução e a realizar configurações referentes às funcionalidades especificadas nos requisitos tecnológicos;

Requisitos Legais, Sociais e Ambientais	
ID	**Descrição**
R.LSA01	A empresa deverá estar habilitada juridicamente (art. 28 da Lei n.º 8.666/93) e em regularidade fiscal e trabalhista (art. 29 da Lei n.º 8.666/93).
R.LSA02	Cumprir o disposto no inciso XXXIII do art. 7.º da Constituição Federal de 1988, quanto ao emprego de menores.
R.LSA03	Promover a correta destinação dos resíduos resultantes da prestação do serviço, tais como peças substituídas, embalagens, entre outros, observando a legislação e princípios de responsabilidade socioambiental como a Política Nacional de Resíduos Sólidos (Lei n.º 12.305/2010) e o Guia de Contratações Sustentáveis da Justiça do Trabalho (Resolução n.º 103/2012 do Conselho Superior da Justiça do Trabalho).

ANEXO II – REQUISITOS E POLÍTICA DE SEGURANÇA

1. A Contratada deverá dar ciência e garantir o pleno cumprimento da política, normas e procedimentos de segurança da informação vigentes no TST.
2. O acesso às instalações do Contratante onde serão realizados os serviços é controlado e permitido somente às pessoas autorizadas.
3. Os profissionais deverão utilizar a conta que lhe for atribuída, de forma controlada e intransferível, mantendo secreta a sua respectiva senha, pois todas as ações efetuadas através desta, serão de responsabilidade do profissional da Contratada.
4. A Contratada deverá garantir a segurança das informações do TST e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido do TST no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.
5. A Contratada deve divulgar aos seus profissionais a Política de Segurança da Informação do TST, PSI-TST, e assegurar-se de sua observação e cumprimento no curso da prestação de serviços no Tribunal. A PSI-TST está formalizada no ATO 764/GDGSET.GP de 27/11/2012, disponível no seguinte endereço eletrônico: http://aplicacao.tst.jus.br/dspace/handle/1939/27977
6. A contratada e seus profissionais devem manter sigilo absoluto sobre documentos elaborados e informações obtidas dentro do TST.
7. Em relação aos requisitos de Confidencialidade, a solução deverá:

    7.1.1 Mascarar senhas e outros campos de entrada sensíveis;

    7.1.2 Não armazenar as senhas em texto claro em *backend*, quando armazenadas devem passar por processo de *hash* com uma função pelo menos equivalente a SHA-256;

    7.1.3 Utilizar SSL nos acessos com informações sensíveis;

    7.1.4 Não utilizar protocolos ou aplicações reconhecidamente inseguros, como FTP, Telnet para comunicação com redes externas.