Pregão Eletrônico

- **Visualização de Recursos, Contrarrazões e Decisões**

CONTRARRAZÃO :

A
FUNDAÇÃO NACIONAL DE SAÚDE - FUNASA

À AUTORIDADE COMPETENTE PARA O JULGAMENTO DOS RECURSOS
ILMA SRª. PREGOEIRA

Edital de Pregão Eletrônico nº 05/2020
Processo nº 25100.012.521/2019-21

ZOOM TECNOLOGIA LTDA., já qualificada nos autos deste procedimento licitatório, respeitosamente, vem apresentar CONTRARRAZÕES ao RECURSO ADMINISTRATIVO interposto pela SOLUCÕES EM TELEINFORMATICA LTDA, igualmente qualificada, apresentando, para tanto, as seguintes razões de fato e de direito.

I. SÍNTESE FÁTICA.

Trata-se de Pregão Eletrônico para a escolha da proposta mais vantajosa para a contratação de switches de acesso 13 com cabos de empilhamento, interfaces de fibra ótica, software d respectivos serviços de instalação e garantia do fabricante para atender as necessidades da FUNASA, conforme edital do Pregão Eletrônico nº 05/2020 realizado no dia 10/07/2020.

A recorrida, na disputa de lances, apresentou o MENOR PREÇO para vir a ser declarada vencedora do Grupo 01 – G1, apresentando a proposta mais vantajosa dentro dos requisitos técnic no instrumento convocatório.

No entanto, apesar de legítima e correta a decisão que a declarou vencedora do certame, a licitante recorrente NTSEC SOLUCÕES, não satisfeita com o correto resultado do julgament Nobre Pregoeira e sua equipe técnica, manifestou sua intenção de recurso, nestes termos:

"Com base no item 11 do edital, viemos por meio deste, tempestivamente, interpor intenção de recurso, motivada pelos itens de requisitos técnicos não atendidos pela empresa vencedora inclusive itens sem comprovação documental."

Ainda que, inconsistente e frágil, esta manifestação não aponta qualquer erro técnico ou jurídico da proposta, somente afirma fatos que restam não comprovados. De todo modo, foram a recursais interpostas pela recorrente.

Ocorre que a recorrente, inconformada, alega equivocadamente a existência de violações aos itens do G1, os quais já foram devidamente analisados por meio de documentação té diligências, suprindo todos os questionamentos suscitados em prol de garantir a maior segurança jurídica ao certame e por comprovar, minuciosamente, o cumprimento de todos especificações técnicas exigidas na proposta mais vantajosa, ofertada pela recorrida.

Neste sentido, as razões recursais da recorrente desmerecem o parecer técnico ao alegar em suas razões que houve descumprimento de requisitos, apesar de comprovadas em doc atendimento. O que por si só já comprova serem estas razões equivocadas tendo em vista que os motivos apresentados foram devidamente esclarecidos à Nobre Pregoeira e sua previamente.

Sendo assim, a injusta provocação da recorrente visa apenas induzir a erro esta Nobre Pregoeira e sua equipe técnica de forma que comprovaremos a ilegalidade das suas razões, uma Tecnologia Ltda atendeu a todas as exigências do instrumento convocatório, conforme será visto a seguir.

II. DA TOTAL IMPROCEDÊNCIA DO RECURSO INTERPOSTO.

Inicialmente, o primeiro ponto que deve ser destacado é o de que o intuito do pregão é obter a proposta mais vantajosa do ponto de vista econômico para a administração, garantind igualdade de direitos aos participantes.

Desse modo, tem-se que a interpretação do edital deve ser feita à luz dessa premissa, de sorte que as obrigações previstas devem ser cumpridas e observadas, porém, afastando-se er casos o entendimento restritivo e literal, sob pena de desvirtuar a própria finalidade do pregão.

Nesse toar, o princípio da vinculação ao edital, que prevê necessidade de se observar o disposto no edital, como já consolidado há muito tempo em nossa jurisprudência, não é absoluto e ser utilizado para restringir a concorrência ou tampouco agredir o bom senso e a lógica, até porque, deve ser aplicado em observância ao princípio da razoabilidade, havendo, pois, uma in os dois.

Para tanto esta douta comissão, atentou-se aos documentos apresentados e considerou como base informações contidas nos documentos técnicos, declarações da própria proponente e s compõem a proposta comercial apresentada para análise final.

Em ato desesperado, insurge-se a recorrente com alegações descabidas, afirmando ter a recorrida não cumprido com as exigências editalícias em sua íntegra, as quais passamos a confro a seguir:

Referente ao "Item 25.10.1.13. Possuir servidor TACACS para autenticação dos operadores e permitir autorização de comandos que podem ou não ser atribuídos ao operador dos dispo (AAA);"

As comprovações e referências apresentadas pela planilha de respostas "Planilha Resposta Ponto-a-Ponto - FUNASA_PE5-2020__v3.xlsx" atrav https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/p_des_authentication_005.html?ft=0&fe=10&hib=4.1.3.1.3&id=p_des_authentication_005&text=Function&docid=EDOC1100107092 na página 21 demonstram claramente que o sistema de gerenciamento eSight possui para autenticação de usuários através da função "Authentication Mode Management e Local authentication", isso quer dizer que além do eSight possui métodos de autenticação atravé externos, tais como, RADIUS, LDAP e SSO também possui o método de autenticação local para quando um usuário digita um nome de usuário e senha para login, o servidor eSight verific informações de login do usuário. Não resta dúvidas de que o sistema eSight possui servidor interno e funcionalidade que permite para autenticação de operadores de dispositivos de r referido item 25.10.1.13.

Ainda na mesma página 21, o sistema de gerência eSight ainda conta com a funcionalidade de "User Management (Gerenciamento de usuários)" que permite o gerenciamento de usuá gerenciamento de direitos do usuário, a consulta de informações on-line do usuário, a configuração de informações pessoais e o gerenciamento de políticas de segurança. Gerenciamento d

• Suporta autenticação de usuário. O administrador de segurança pode atribuir direitos diferentes a diferentes funções de usuário com base no plano de serviço, melhorando a eficié melhorando a segurança do sistema.
• Permite que um usuário consulte informações on-line do usuário e entra no modo de usuário único.
• Permite que um usuário defina informações pessoais, como alterar uma senha e modificar as informações de contato.
• Fornece políticas de segurança, como políticas de configuração de conta, políticas de senha, políticas de controle de acesso baseadas em endereço IP e políticas de tempo de login.
o Configuração de diretiva de conta = Políticas de conta são políticas com o tamanho mínimo de nome de usuário e relacionadas ao login do usuário. Uma diretiva de conta apropriada p segurança de acesso ao sistema.
o Configuração de política de senha = As diretivas de senha definem a complexidade da senha, o período de atualização e as restrições de caracteres. Uma política de senha de usuário a impedir que os usuários definam senhas bastante simples ou retenham senhas por um longo período, aprimorando a segurança de acesso ao sistema.
o Configuração de políticas de controle de acesso baseadas em endereço IP = Defina o intervalo de endereços IP no qual o eSight pode efetuar login. Um usuário vinculado a esse interva IP pode efetuar login no eSight apenas a partir de endereços IP nesse intervalo.
o Configuração da política de tempo de login = Defina o tempo durante o qual o eSight pode efetuar login. Um usuário vinculado a esta política de horário de login pode efetuar login no e horário especificado na política.

A segunda comprovação referenciada através do link https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/feature_ft=0&fe=10&hib=7.1.3.3&id=feature_auth_002&text=User%2520Authorization&docid=EDOC1100107092 na página 1522 conforme documento Hedex oficial do fabricante, vem der sistema de gerência eSight ofertado ainda dispõe da funcionalidade de "Autorização de Usuários (User Authorization)" que especifica quem pode executar e quais operações em quais operações que os usuários podem executar em objetos variam de acordo com seus direitos e configurações. conforme documento Hedex oficial do fabricante, vem demonstrar que o siste eSight ofertado ainda dispõe da funcionalidade de "Autorização de Usuários (User Authorization)" que especifica quem pode executar e quais operações em quais dispositivos. As op usuários podem executar em objetos variam de acordo com seus direitos e configurações.

Vendo a Tabela 1 da figura acima, pode-se constatar de forma clara através da coluna "Function Scenario" alguns exemplos de perfis de vários tipos de usuários criados na base de dad que estão associados respectivamente ao seu "Direitos de operação (Operation rights)", ou seja, os perfis, usuários, operações e direitos são customizáveis atendendo aos mais diversos ti

Complementando ainda nessa página 1522 através do mesmo link, é demonstrado através da Figura 2 um exemplo onde diversos usuários possuem perfis e autorizações distintas para de rede.

Através da Tabela 2, constata-se que o foram criados 3 perfis, sendo "Administrators, Alarm monitoring of City A e Alarm monitoring of City B", e que usuários classificados como adminis gerenciar os dispositivos das "City A e City B" e sem restrição de comandos. Os usuários classificados como "Alarm monitoring of City A" só podem gerenciar os dispositivos da "City comandos de "Browse Current Alarms, Browse Masked Alarms, Browse Historical Alarms e Browse Events" podem ser executados.

Não resta dúvidas de que o sistema eSight possui servidor interno e funcionalidade de permitir autorização de comandos que podem ou não ser atribuídos ao operador dos dispositivos de o referido item 25.10.1.13.

É importante destacarmos que em resposta aos diversos questionamentos publicados no dia 29/05/2020 às 9:10:26, vide abaixo, soluções similares do protocolo TACACS foram devidame e permitidas pela FUNASA, não deixando dúvidas que soluções similares ao protocolo TACACS seriam aceitas, como é o caso do sistema eSight que possui servidor interno para autorização de comandos para os operadores dos dispositivos da rede.

Resposta 29/05/2020 09:10:26:
Questionamento 1: Entendemos que serão aceitas soluções similares para autenticação dos operadores dos dispositivos de rede (AAA) conforme requisito publicado na versão anteri
Referência item ´25.10.1.13-Possuir servidor TACACS ou similar para autenticação dos operadores dos dispositivos de rede (AAA);", grifo nosso, ao evento de suspensão do pregão a
4/Maio/2020, onde não havia impedimento da nossa participação na licitação. Está correto nosso entendimento?
Resposta 01: Será aceito servidor similar ao TACACS para autenticação dos operadores dos dispositivos de rede (AAA) desde que possua a mesma performance da solução TACACS.
A empresa NTSEC ainda interpreta de forma totalmente equivocada e leviana a respeito da compatibilidade entre os protocolos HWTACACS e TACACS/TACACS+. A informação de incc
restrita aos atributos proprietários da Cisco, porque diferentes fornecedores definem campos e significados diferentes para atributos proprietários. Um ato desesperado da recorrente e
processo.

Desta forma apresentaremos do entendimento correto da funcionalidade de HWTACACS. O HWTACACS é o nome comercial usado pelo fabricante Huawei para a imp
funcionalidade/protocolo chamada popularmente de TACACS e que evidenciamos através do documento "Planilha Resposta Ponto-a-Ponto - FUNASA_PE5-2020__v3.xlsx" a
https://support.huawei.com/hedex/pages/EDOC1100126530AEI02128/02/EDOC1100126530AEI02128/02/resources/dc/dc_fd_aaa_0017.html?
ft=0&fe=10&hib=4.2.12.2.2.5.1&id=ENUS_CONCEPT_0176366149&text=Overview%2520of%2520HWTACACS&docid=EDOC1100126530 na página 6171 para comprovação do "item 2
implementar TACACS/TACACS+ ou similar para gerenciamento do dispositivo;" para os Switches Tipo 1 e Switches Tipo 2.

O HWTACACS é um protocolo de troca de informações que usa o modelo cliente / servidor para fornecer validação centralizada de usuários que tentam acessar seus dispositivos. Usa o TC
Control Protocol) e o número da porta TCP 49 para transmitir dados. O HWTACACS fornece autenticação, autorização e contabilidade independentes para usuários que acessam a Interr
protocolo ponto a ponto (PPP) ou da rede dial-up privada virtual (VPDN) e para administradores. Como um aprimoramento para o TACACS (RFC 1492). O HWTACACS é compatível com
Cisco. Os switches da Huawei podem funcionar como clientes HWTACACS para trabalhar com servidores TACACS + para implementar o AAA. Por exemplo, um switch executando o HWT
comunicar com um servidor Cisco (como o ACS). No entanto, o HWTACACS pode não ser compatível com os atributos proprietários da Cisco, porque diferentes fornecedores def
significados diferentes para atributos proprietários.

HWTACACS e RADIUS têm as seguintes características:
• Modelo Cliente / Servidor
o Cliente HWTACACS: geralmente reside no servidor de acesso à rede (NAS) e pode residir em toda a rede. O cliente é responsável por transmitir informações do usuário para o servi
especificado e, em seguida, executa operações de acordo com as informações retornadas pelo servidor.
o Servidor HWTACACS: geralmente é executado no computador central ou na estação de trabalho. O servidor mantém informações de autenticação e acesso à rede do usuário e é r
receber solicitações de conexão, autenticar usuários e retornar as informações necessárias aos clientes.
• Chave de compartilhamento usada para criptografar informações do usuário
• Boa escalabilidade.
Não há dúvida quanto à compatibilidade entre os Protocolos HWTACAS e TACACS/TACACS+ até porque a implementação do HWTACACS é baseada na "RFC1492" (An Access Control Proto
Called TACACS - https://tools.ietf.org/html/rfc1492) e no "draft-grant-tacacs-02 TACACS+" (The TACACS+ Protocol Version 1.78 - https://tools.ietf.org/html/draft-grant-tacacs-02).

Sendo assim estamos atendendo em sua totalidade o item 25.10.1.13.

Referente ao "Item 25.10.1.15. Deverá prover a visibilidade dos dispositivos da rede, além dos dispositivos físicos que estão autenticando na rede, dando visibilidade inclusive do siste
destes dispositivos (Windows, Linux, IOS, etc);"

A recorrente insiste em alegações infundadas na tentativa desesperada de desqualificar nossa proposta que foi a mais vantajosa para a FUNASA.

Apresentamos as comprovações e referências através da planilha de respostas "Planilha Resposta Ponto-a-Ponto - FUNASA_PE5-2020__v3.xlsx"
link:https://support.huawei.com/hedex/pages/EDOC1000183850JEG12297/12/EDOC1000183850JEG12297/12/resources/enus_topic_0087856711.html?
ft=0&fe=10&hib=4.1.3.12.4&id=ENUS_TOPIC_0087856711&text=Single%2520NE%2520Management&docid=EDOC1000183850, vide figura abaixo, com evidência de que o sistema de
monitora o dispositivo de rede com possibilidade de visualização de diversas informações acerca do dispositivo, não apenas versão (sistema operacional do dispositivo) e modelo mas tamb
a visão geral do dispositivo, incluindo o nome do dispositivo, nome do host, status do dispositivo, versão, número de série, último horário de sincronização, último horário de inicializ
autenticação de AP, modelo, endereço IP, endereço MAC, horário da última alteração de configuração, KPIs de desempenho, principais alarmes e tráfego de interface.

O que já demonstra atendimento ao referido item 25.10.1.15.

Além disso complementamos com outra evidência através do
https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/p_des_resource_005.html?
ft=0&fe=10&hib=4.1.3.2.3&id=p_des_resource_005&text=Function&docid=EDOC1100107092, na página 27, também informado na planilha de respostas "Planilha Resposta P
FUNASA_PE5-2020__v3.xlsx", trazendo clareza quanto algumas funções do sistema eSight quanto ao gerenciamento de recursos fornecendo vários métodos para descobrir dispositivos e
sistema.
• Os dispositivos podem ser adicionados ao eSight após serem descobertos, adicionados manualmente um a um ou importados em lotes usando um arquivo do Excel.
• Os dispositivos podem ser descobertos automaticamente com base no segmento de rede, ARP ou roteamento.
• Os dispositivos podem ser gerenciados por grupo. Os usuários podem criar, visualizar, modificar e excluir um grupo de dispositivos.
• Os dispositivos também podem ser descobertos e adicionados automaticamente ao eSight usando modelos de protocolo.
• As tarefas de descoberta de dispositivos podem ser gerenciadas da seguinte maneira:
o Veja todas as tarefas de descoberta automática na lista de tarefas, incluindo tarefas únicas e periódicas.
o Veja os resultados de todas as tarefas de descoberta automática e informações básicas sobre dispositivos descobertos.
o Defina um segmento de endereço IP ou endereços IP específicos de dispositivos excluídos.
Monitoramento de Recursos
• Os usuários podem visualizar informações básicas sobre dispositivos, incluindo os protocolos que eles usam.
• As informações do dispositivo podem ser exportadas para ajudar os usuários a aprender sobre os detalhes do dispositivo.

Ainda assim, com intuito de elucidar ainda mais, através documento Hedex do sistema de gerência eSight utilizado em grande parte das comprovações,
https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/p_des_topology_005.html?
ft=0&fe=10&hib=4.1.3.4.3&id=p_des_topology_005&text=Function&docid=EDOC1100107092, na página 39, temos na figura 1, vide abaixo, a visibilidade dos dispositivos da rede
topologia.

Outra referência de comprovação para o item 25.10.1.15 pode ser obtido também e de forma clara através documento Hedex do sistema de gerência eSight utilizado em grande parte das
temos a funcionalidade de "Terminal
Management",link:https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/n_product_description_terminal1.html?
ft=0&fe=10&hib=7.1.12.2.1.1&id=n_product_description_terminal1&text=Definition&docid=EDOC1100107092

O eSight fornece informações detalhadas sobre terminais de acesso (dispositivos de rede) e oferece uma abordagem unificada para você gerenciar terminais de acesso. O eSight forn
acesso ao terminal, logs suspeitos de terminal, gerenciamento de acesso não autorizado e notificação remota para permitir que os administradores de rede obtenham informações de ace
em tempo real.
Explorando ainda a funcionalidade do "Terminal Resource Management", através do
https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/n_product_description_terminal4.html?
ft=0&fe=10&hib=7.1.12.2.1.2&id=n_product_description_terminal4&text=Functions&docid=EDOC1100107092.

Veja abaixo na Figura 4 abaixo, algumas das informações de visibilidade dos dispositivos que ser conectaram a rede.

Functions
eSight provides detailed information about access terminals and offers a unified approach for you to manage access terminals. eSight provides terminal access history, suspicious
unauthorized access management, and remote notification to allow network administrators to obtain terminal access information in real time.
Terminals that have accessed the network can be discovered either by a manually conducted immediate discovery or a periodically conducted automatic discovery.
Terminal Discovery Configuration
• Whether to parse terminal names.
• Whether to enable MAC address deduplication.
• Whether to enable automatic discovery.
• Intervals of automatic discovery.
• Discovery scope, which applies to both immediate discovery and automatic discovery.

Figure 1 Terminal discovery settings
Whitelist
You can configure a whitelist that contains authorized IP addresses and MAC addresses. When the configuration takes effect, eSight checks whether a discovered terminal is authorized
records its details for you to acknowledge the unauthorized terminal.
Figure 2 Setting the whitelist

Access Binding Rule
You can configure Port-IP or Port-MAC rules to restrict access terminals under device ports. Yon can also configure IP-MAC rules to restrict binding relationships between IP and MAC ad
identifies terminals that break these rules as unauthorized terminals and records detailed access information.
Figure 3 Access binding rule

Terminal Access Record
• View terminal access details and access history.
• View unauthorized access logs of terminals.
• Switch to the physical topology to locate the access devices of terminals.
• Switch from an access interface to the Interface Management page.
• Switch to the device panel to view the access interfaces of terminals.
• Configure terminal remarks.
Figure 4 Terminal access record

Suspicious Terminal Report

• Check invalid MAC addresses to detect unauthorized terminal access.
• Check duplicate MAC addresses to detect MAC address theft.
• Check duplicate IP addresses to detect IP address theft.
Figure 5 Suspicious terminal

Unauthorized Access
eSight detects unauthorized terminal access based on the IP and MAC address whitelists configured. With unauthorized access management, you can:
• View unauthorized access logs and unauthorized terminal details.
• Export unauthorized terminal details.
• Acknowledge unauthorized terminals.
Figure 6 Unauthorized access record

Remote Notification
You can configure eSight to send an email notification upon detecting unauthorized terminal access.
Figure 7 Remote notification

É importante destacarmos que em resposta aos diversos questionamentos feitos acerca do referido item, sabiamente a FUNASA suspendeu o pregão 4/2020 motivado pela correção e es item 25.10.1.15 quanto a necessidade ou não do escopo de uma solução de NAC para o sistema de gerência Item 5 do edital.

Diante do exposto fica claro o atendimento em sua totalidade do item 25.10.1.15 e o desconhecimento profundo da recorrente na solução do sistema de gerência eSight e além da alega da necessidade da solução Agile Controller do fabricante Huawei.

Referente ao "Item 25.10.1.25. Permitir a monitoração de uso de energia PoE em cada porta e consolidado para cada equipamento;"

A recorrente desconhece a solução do fabricante Huawei e faz insinuações quanto ao atendimento. Vamos aos fatos. A referência apontada como comprovação para o item 25.10.1.25 https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/n_httpclient_inter02_07.html?ft=0&fe=10&hib=8.1.3.3.4.8&id=n_httpclient_inter02_07&text=Performance%2520Indicator%2520List&docid=EDOC1100107092, página 3680 do documento planilha de respostas "Pl Ponto-a-Ponto - FUNASA_PE5-2020__v3.xlsx" mostra alguns indicadores de customizáveis que podem ser configurados a partir da funcionalidade "Performance Management" da plataforma na tabela abaixo a existência de indicadores que são coletados através de MIBs dos equipamentos para que o monitoramento ou relatório ou dashboard ou visualização pode ser obtida. F indicadores de consumo de PoE por porta existem e que podem ser coletados para o devido monitoramento.

Desta forma introduziremos a funcionalidade de "Gerenciamento de Performance – Performance Management" que permite monitorar diversos indicadores dos elementos de redes g eSight., através do link https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/n_des_pe ft=0&fe=10&hib=7.1.6.1.2&id=n_des_perf_005_0&text=Function&docid=EDOC1100107092s, página 1597.

A funcionalidade de gerenciamento de desempenho fornece funções como monitoramento de gerenciamento de políticas, gerenciamento de dados de desempenho e Meus Favoritos.
Monitorando o gerenciamento de políticas
A política de monitoramento inclui o objeto monitorado, o indicador de monitoramento e o período de coleta e o limite dos indicadores de monitoramento. O administrador pode conf flexível políticas de monitoramento para diferentes cenários de monitoramento.
• Define indicadores comuns do mesmo tipo de dispositivo que um modelo de indicador. Quando uma tarefa de coleta de desempenho é criada, o modelo de indicador pode ser carrega implementando a configuração rápida de indicadores de coleta para dispositivos especificados.
• Define o limite do indicador de desempenho. Quando um indicador atinge o limite, o eSight gera um alarme.
• Adiciona, exclui, inicia, para e modifica tarefas de coleta de desempenho.
• Exibe informações de coleta de indicadores intuitivamente, especifica se um indicador é coletado diretamente na tabela, define o limite de coleta de indicadores.
Gerenciamento de dados de desempenho
Na página de visão geral dos dados de desempenho, você pode gerenciar dados de desempenho de vários recursos, incluindo:
• Exibindo dados de desempenho em uma curva
• Definindo condições para consultar dados de desempenho
• Exportando o resultado da consulta para um arquivo .xls
• Exportando o resultado da consulta para um arquivo de imagem
• Adicionando dados de desempenho diretamente à pasta Favoritos para consulta subsequente

Veja na figura abaixo alguns exemplos de monitoração, porém é claro que não mostrará todos os indicadores disponíveis como exemplos em gráficos, mas logo adiante veja a possibilidad uma tarefa de monitoração onde é possível escolher os indicadores, e é exatamente onde entra os indicadores demostrados na referência das comprovações onde é possível customizar o acordo com as necessidades do cliente.

Agora demostraremos através do "Performance Management" o processo de criação de uma tarefa de monitoração de desempenho com a possibilidade de escolher os tipos de indic monitorados, onde por exemplo pode ser os indicadores demonstrados de consumo de PoE por porta, veja através https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/eSight_hlp_perf_003_1.html?ft=0&fe=10&hib=7.1.6.3&id=eSight_hlp_perf_003_1&text=Creating%2520a%2520Performance%2520Task&docid=EDOC1100107092, página 1601.

Veja no passo 4 (quatro) o momento onde o indicador pode ser escolhido. Neste caso os indicadores da planilha

Creating a Performance Task
1. Choose Performance > Monitoring Template from the main menu.

2. Select a resource type in the navigation tree on the left, click Create in the area on the right, and create a monitoring template in the dialog box that is displayed.
3. Choose Performance > Monitoring Settings from the main menu.
4. Select a resource type from the navigation tree on the left and click Create in the area on the right. On the page that is displayed, create a performance collection task. When se indicators, you can select templates or add indicators.
After you finish creating a performance data collection task, you can view data on the Performance Data page after two data collection periods. For example, if the data collection period minutes, you are advised to view data on the Performance Data page after 10 minutes.
Parent Topic: Performance Management Copyright © Huawei Technologies Co., Ltd.< Previous topicNext topic >

Ressaltamos, que a evidência inicialmente apontada por nós deixa claro que os indicadores contidos na planilha "Performanceindicatorlist.xls" são adicionais e que podem ser utilizado tarefas de monitoramento de desempenho através da funcionalidade "Performance Managemnt" explicada anteriormente. Veja no texto marcado abaixo, lembrando que essa foi a com apontado pela recorrida.

Mesmo diante de tantos fatos demonstrados de que o sistema de gerenciamento eSight atende ao requisito, apresentaremos outra evidência real com "prints" de tela da plataforma eSigh o consumo de PoE (power over ethernet) de switches gerenciados pelo eSight. Veja abaixo:

1- Consumo do PoE total do Switch
Resource □ Network □ Network Device

Seleciona o Switch

View □ Power Management

2- Consumo do PoE por interface
Performance □ Monitoring Settings

Criar uma nova tarefa para coleta de dados de consumo do PoE
Network Device □ Interface □ Create

Definindo parâmetros de coleta

Verificar resultado da coleta
Clicar em "Query Performance Data"

Na figura abaixo veja as informações de consumo de PoE por porta do switch e perceba que o indicador utilizado é o mesmo apontado pela tabela de "performanceindicatorlist.xls"

3 - Consumo do PoE por interface - Método Via MIB Browser
Resource □ Network □ Network Device

Seleciona o Switch

MIB Browser

Obter informação via MIB
1.3.6.1.4.1.2011.5.25.195.3.1.10
hwPoePortConsumingPower
Consumo medido em mW (milliwatts)

Não resta dúvida que a solução atende integralmente ao requisito item 25.10.1.25.

Referente ao "Item 25.10.1.26. Permitir a monitoração de temperatura de operação dos equipamentos;"

A recorrente desconhece a solução do fabricante Huawei e faz insinuações quanto ao atendimento. Vamos aos fatos. A referência apontada como comprovação para o item 25.10.1.26 https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/n_httpclient_inter02_07.html?ft=0&fe=10&hib=8.1.3.3.4.8&id=n_httpclient_inter02_07&text=Performance%2520Indicator%2520List&docid=EDOC1100107092, página 3680 do documento planilha de respostas "Pl Ponto-a-Ponto - FUNASA_PE5-2020__v3.xlsx" mostra alguns indicadores de customizáveis que podem ser configurados a partir da funcionalidade "Performance Management" da plataforma na tabela abaixo a existência de indicadores que são coletados através de MIBs dos equipamentos para que o monitoramento ou relatório ou dashboard ou visualização pode ser obtida. F indicadores de temperatura existem e que podem ser coletados para o devido monitoramento.

Desta forma introduziremos a funcionalidade de "Gerenciamento de Performance – Performance Management" que permite monitorar diversos indicadores dos elementos de redes g eSight., através do link https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/n_des_pe ft=0&fe=10&hib=7.1.6.1.2&id=n_des_perf_005_0&text=Function&docid=EDOC1100107092s, página 1597.

A funcionalidade de gerenciamento de desempenho fornece funções como monitoramento de gerenciamento de políticas, gerenciamento de dados de desempenho e Meus Favoritos.
Monitorando o gerenciamento de políticas.
A política de monitoramento inclui o objeto monitorado, o indicador de monitoramento e o período de coleta e o limite dos indicadores de monitoramento. O administrador pode conf flexível políticas de monitoramento para diferentes cenários de monitoramento.
• Define indicadores comuns do mesmo tipo de dispositivo que um modelo de indicador. Quando uma tarefa de coleta de desempenho é criada, o modelo de indicador pode ser carrega implementando a configuração rápida de indicadores de coleta para dispositivos especificados.
• Define o limite do indicador de desempenho. Quando um indicador atinge o limite, o eSight gera um alarme.
• Adiciona, exclui, inicia, para e modifica tarefas de coleta de desempenho.
• Exibe informações de coleta de indicadores intuitivamente, especifica se um indicador é coletado diretamente na tabela, define o limite de coleta de indicadores.
Gerenciamento de dados de desempenho.
Na página de visão geral dos dados de desempenho, você pode gerenciar dados de desempenho de vários recursos, incluindo:
• Exibindo dados de desempenho em uma curva
• Definindo condições para consultar dados de desempenho
• Exportando o resultado da consulta para um arquivo .xls
• Exportando o resultado da consulta para um arquivo de imagem
• Adicionando dados de desempenho diretamente à pasta Favoritos para consulta subsequente

Veja na figura abaixo alguns exemplos de monitoração, porém é claro que não mostrará todos os indicadores disponíveis como exemplos em gráficos, mas logo adiante veja a possibilidad uma tarefa de monitoração onde é possível escolher os indicadores, e é exatamente onde entra os indicadores demostrados na referência das comprovações onde é possível customizar o acordo com as necessidades do cliente.

Agora demostraremos através do "Performance Management" o processo de criação de uma tarefa de monitoração de desempenho com a possibilidade de escolher os tipos de indic monitorados, onde por exemplo pode ser os indicadores demonstrados de consumo de PoE por porta, veja através https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/eSight_hlp_perf_003_1.html?ft=0&fe=10&hib=7.1.6.3&id=eSight_hlp_perf_003_1&text=Creating%2520a%2520Performance%2520Task&docid=EDOC1100107092, página 1601.

Veja no passo 4 (quatro) o momento onde o indicador pode ser escolhido. Neste caso os indicadores da planilha.

Creating a Performance Task
5. Choose Performance > Monitoring Template from the main menu.

6. Select a resource type in the navigation tree on the left, click Create in the area on the right, and create a monitoring template in the dialog box that is displayed.
7. Choose Performance > Monitoring Settings from the main menu.

8. Select a resource type from the navigation tree on the left and click Create in the area on the right. On the page that is displayed, create a performance collection task. When set indicators, you can select templates or add indicators.
After you finish creating a performance data collection task, you can view data on the Performance Data page after two data collection periods. For example, if the data collection period minutes, you are advised to view data on the Performance Data page after 10 minutes.
Parent Topic: Performance Management Copyright © Huawei Technologies Co., Ltd.< Previous topicNext topic >

Ressaltamos, que a evidência inicialmente apontada por nós deixa claro que os indicadores contidos na planilha "Performanceindicatorlist.xls" são adicionais e que podem ser utilizado tarefas de monitoramento de desempenho através da funcionalidade "Performance Managemnt" explicada anteriormente. Veja no texto marcado abaixo, lembrando que essa foi a com apontado pela recorrida.

Mesmo diante de tantos fatos demonstrados de que o sistema de gerenciamento eSight atende ao requisito, apresentaremos outra evidência real com "prints" de tela da plataforma eSigh o monitoramento de temperatura de switches gerenciados pelo eSight. Veja abaixo:

Na figura abaixo veja as informações de temperatura do switch e perceba que o indicador utilizado é o mesmo apontado pela tabela de "performanceindicatorlist.xls"

1- Método 1 (MIB Browser)
Resource Network Network Device

Seleciona o Switch
MIB Browser
Obter informação via MIB
hwEntityTemperature (1.3.6.1.4.1.2011.5.25.31.1.1.1.1.11)
Medida em graus Celsius (neste exemplo está em 47)

2- Método 2 (Device Panel)
Resource Network Network Device

Seleciona o Switch

Escolha a opção "Device Panel"

Clicar com o botão direito do mouse sobre os leds de status no lado esquerdo do equipamento.

Clicar na opção "View Board Temperature"

3 - Método 3 (Performance Task)
Via Performance Task
Performance Monitoring Settings

Criar uma nova tarefa para coleta de dados de temperatura
Network Device Slot Create

Definindo parâmetros de coleta

Verificar resultado da coleta
Clicar em "Query Performance Data"

Não resta dúvida que a solução atende integralmente ao requisito item 25.10.1.26.

Referente ao "Item 25.7.2.13 Deve ser suportada a atribuição de VLANs após a identificação do usuário, atribuição do usuário a uma VLAN "Guest" caso a máquina que esteja utilizand Rede não tenha cliente 802.1x operacional. Caso ocorra falha de autenticação de um usuário com um cliente 802.1x operacional o mesmo deverá ser alocado em uma VLAN "q características próprias;"

Novamente a recorrente mostra total desconhecimento técnico acerca das funcionalidades exigidas no edital, não há qualquer ligação plausível entre o requisito do item 25.7.2.13 com o li funcionalidades dos equipamentos switches S5731-S do fabricante Huawei. Um ato de desepero com apenas o intuito de retardar o andamento do processo e prejudicar o planejamento de

Primeiro, o requisito do item 25.7.2.13 é muito claro em solicitar a funcionalidade de "VLAN GUEST", para isso demonstramos através da referência apontada como comprovação para o através do link https://support.huawei.com/hedex/pages/EDOC1100126530AEI02128/02/EDOC1100126530AEI02128/02/resources/dc/dc_cfg_ ft=0&fe=10&hib=4.2.12.4.7.14&id=ENUS_TASK_0176369212&text=(Optional)%2520Configuring%2520the%2520Guest%2520VLAN%2520Function&docid=EDOC1100126530, página documento planilha de respostas "Planilha Resposta Ponto-a-Ponto - FUNASA_PE5-2020__v3.xlsx" que os switches ofertados S5731-S possuem, suportam e implementam a funcional GUEST".

Vamos além e complementaremos com outra referência ainda a partir do mesmo documento Hedex disponibilizado em nossa proposta, veja que os switches S5731-S também implem métodos, sendo "VLAN RESTRICT" para os casos de falha na autenticação 802.1x e são redirecionados para outra VLAN para, por exemplo atualização do anti-vírus. A

https://support.huawei.com/hedex/pages/EDOC1100126530AEI02128/02/EDOC1100126530AEI02128/02/resources/dc/dc_cfg_nac_0020.html?ft=0&fe=10&hib=4.2.12.4.7.15&id=ENUS_TASK_0176369213&text=(Optional)%2520Configuring%2520the%2520Restrict%2520VLAN%2520Function&docid=EDOC1100126530, página 6

E o outro, sendo "VLAN CRITICAL", durante a autenticação 802.1X, quando o dispositivo de acesso é desconectado do servidor de autenticação ou o servidor de autenticação falha, autenticação na rede é interrompido.. Através do link https://support.huawei.com/hedex/pages/EDOC1100126530AEI02128/02/EDOC1100126530AEI02128/02/resources/dc/dc_cfg_ ft=0&fe=10&hib=4.2.12.4.7.16&id=ENUS_TASK_0176369214&text=(Optional)%2520Configuring%2520the%2520Critical%2520VLAN%2520Function&docid=EDOC1100126530, página 64

Segundo, veja na referência abaixo que as funcionalidades de NAC (802.1x, MAC Authentication, Portal Authentication) NÃO SÃO CONTROLADAS POR LICENÇA. Já fazem parte do softwar restrição ou limitação. Link https://support.huawei.com/hedex/pages/EDOC1100126530AEI02128/02/EDOC1100126530AEI02128/02/resources/dc/dc_cfg_nac_ ft=0&fe=10&hib=4.2.12.4.4&id=ENUS_TASK_0177110555&text=Licensing%2520Requirements%2520and%2520Limitations%2520for%2520NAC%2520Common%2520Mode&docid=EDO página 6422.

E por fim, a alegação descabida da recorrente quanto ao licenciamento de VXLAN e N1. Esclarecemos que apesar de ser a única funcionalidade a ser disponibilizada através lice funcionalidade de VXLAN não é escopo dos requisitos técnicos deste edital. Já as licenças de N-1 referem-se exclusivamente a solução de CloudCampus (NaaS) da Huawei que permite g serviços de rede em nuvem. Vide abaixo prints tirados a partir do documento Brochure dos Switches S5731-S disponibilizados em nossa p https://e.huawei.com/en/material/networking/6319b814d3df471cbc466175ecb5a955

Não resta dúvida que a solução atende integralmente ao requisito item 25.7.2.13.

Referente ao "Item 25.10.1.6.1 Caso o fabricante não possua solução de gerenciamento em software (virtualizada) será aceito solução em appliance externo que implemente todas as solicitadas neste termo."

A recorrente insiste na tentativa a qualquer custo inclusive sob alegações equivocadas a respeito de nossa proposta que é a mais vantajosa. As comprovações apresentadas refe 25.10.1.6.1 através da planilha de respostas "Planilha Resposta Ponto-a-Ponto - FUNASA_PE5-2020__v3.xlsx" através https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/enus_topic_0140434736.html?ft=0&fe=10&hib=4.1.7.1&id=ENUS_TOPIC_0140434736&text=Hardware%2520and%2520Software%2520Configurations&docid=EDOC1100107092, página 274 apontam para "physical m solução já vem pré-instalada, o que, significa que o sistema de gerência eSight é um appliance e que não é vendido sem o seu hardware específico o que corrobora com a nota destac hardware do fabricantes Huawei são suportados.

Ao final da mesma página referenciada é demonstrada quais tipos de hardware podem acompanhar o sistema de gerência eSight. Esclarecemos que o sistema de gerência eSight appliance acompanha obrigatoriamente seu respectivo hardware e que a nossa proposta comtempla todos os acessórios, sistemas, licenças necessárias para o funcionamento do eSight pa todos os equipamentos escopo deste edital.

Sendo assim, estamos atendendo ao requisito do item 25.10.1.6.1 do edital, em sua totalidade.
Referente ao "Item 25.10.1.10 Permitir configuração e Zero Touch Provisioning (ZTP);"

Através do mesmo documento "eSight Product Documentation Hedex"utilizado em grande parte das comprovações do item 5, veja na página link:https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/n_product_description_zero4.html?ft=0&fe=10&hib=7.1.12.6.1.2&id=n_product_description_zero4&text=Functions&docid=EDOC1100107092, a funcionalidade de ZTP suportada e presente no sistema de gerência eSight.

Functions
After new switches and routers meeting zero-touch provisioning conditions are installed and powered on, they start the zero touch provisioning process to automatically load syste configuration files, software version packages, and patch files. The network administrator does not need to commission the switches and routers on site.
Making Required Files
After required files including configuration templates, software version packages, patch files, and license files are made, eSight can match required files with devices to implement topolog device ID-based deployment.

Figure 1 Making required files

Topology Plan-based Deployment
eSight allows users to draw and modify network topologies and matches and delivers required files to deploy unconfigured devices.

Figure 2 Topology planning

Figure 3 File matching

Figure 4 Topology comparison

Figure 5 Device deployment

Device ID-based Deployment
Users can create devices, match required files, and then perform deployment and activation operations to deploy unconfigured devices by the MAC address or ESN. S switches c automatically or manually. CE switches and AR routers are activated automatically by default.

Figure 6 Creating devices

Figure 7 Matching required files

Figure 8 Deploying devices

Figure 9 Activating devices

Short Message-based Deployment
Users can create undeployed devices, match deployment files, and send short messages to implement short message-based deployment.

Figure 10 Creating undeployed devices

Figure 11 Matching deployment files

Figure 12 Sending short messages

Zero Touch Re-provisioning
Users can redeploy faulty devices in the physical topology using configuration files of faulty devices or ZTP templates.

Figure 13 Zero touch re-provisioning entrance

Figure 14 Zero touch re-provisioning configuration

Figure 15 Zero touch re-provisioning task

Outra referência da funcionalidade de ZTP no eSight, veja no mesmo documento um exemplo de configuração da funcionalidade de ZTP no si https://support.huawei.com/hedex/pages/EDOC1100107092JEH0704L/09/EDOC1100107092JEH0704L/09/resources/n_zero_conf06_01.html?ft=0&fe=10&hib=7.1.12.6.5.1&id=n_zero_conf06_01&text=Example%2520for%2520Implementing%2520Topology-based%2520Zero%2520Touch%2520Provisioning%2520for%2520the%2520Campus%2520Headquarters&docid=EDOC1100107092, página 2154.
Example for Implementing Topology-based Zero Touch Provisioning for the Campus Headquarters
This section describes how to use the topology to implement zero-touch provisioning for the campus headquarters.
Prerequisites
• The root device and devices to be deployed support zero touch provisioning. For details about device types, see eSight Function List.
• Onsite engineers have installed device hardware based on the topology plan.
• Basic configuration has been completed for a root device and the root device has been added to eSight for management and can communicate normally with eSight through SNMP and Te
• Input or output is not allowed on console interfaces during zero touch provisioning.
• (Optional) The device software package, license file, and patch file have been prepared and uploaded to eSight.
Networking Requirements
On the wired campus network of company M, there are lots of devices at the aggregation and access layers. Traditionally, the network design, and software/hardware installation and cor performed by different personnel. Each device to be deployed needs to be manually associated with provisioning files through a USB flash drive. The configuration is complex and has low the network administrator of the company, requires that eSight implement unified zero touch provisioning for aggregation and access devices to reduce management cost.
In the following figure, the red circle specifies the devices to be deployed.

Figure 1 Implementing topology-based zero touch provisioning for the campus headquarters

Configuration Roadmap
The configuration roadmap is as follows:
1. Configure the root device as a DHCP server and configure the interface for connecting to lower-layer devices.
2. Create device files to be deployed.

3. Create a deployment task.
4. Plan the network topology through topology deployment.
5. Match device files for the devices to be deployed.
6. Clean up configurations for the devices to be deployed and restart the devices.
7. Compare topologies.
8. Trigger and start the deployment based on the topology plan.
Data Plan

Procedure
1. Configure the root device as a DHCP server and configure the interface for connecting to lower-layer devices.
2. system-view
3. [Device] dhcp enable
4. [Device] ip pool dhcp_server //dhcp_server indicates the name of the global address pool.
5. [Device-ip-pool-dhcp_server] network 10.137.58.0 mask 255.255.255.0 //10.137.58.0 is the scope of IP addresses to be assigned to the device for which zero-touch provisioning is to b
6. [Device-ip-pool-dhcp_server] gateway-list 10.137.58.1 //10.137.58.1 is the egress gateway address of the DHCP client.
7. [Device-ip-pool-dhcp_server] option 148 ascii ipaddr=10.137.58.8;port=32175 //10.137.58.8 is the eSight IP address. If southbound and northbound services are separated for eSigh
address here refers to the southbound IP address.
8. [Device-ip-pool-dhcp_server] quit
9. [Device] vlan batch 25 to 30
10. [Device] interface vlanif 25 //VLAN25 is the management VLAN of zero touch deployment.
11. [Device-Vlanif25] ip address 10.137.58.1 255.255.255.0 //10.137.58.1 is the IP address of VLANIF25, which is used as the egress gateway address of the DHCP client.
12. [Device-Vlanif25] dhcp select global
13. [Device-Vlanif25] quit
14. [Device] interface GigabitEthernet 0/0/1 //Configure the interface GE0/0/1 for connecting the root device to the lower-layer device.
15. [Device-GigabitEthernet0/0/1] port link-type trunk
16. [Device-GigabitEthernet0/0/1] port trunk pvid vlan 30
17. [Device-GigabitEthernet0/0/1] port trunk allow-pass vlan 30
18. [Device-GigabitEthernet0/0/1] quit
19. [Device] interface GigabitEthernet 0/0/2 //Configure the interface GE0/0/2 for connecting the root device to the lower-layer device.
20. [Device-GigabitEthernet0/0/2] port link-type trunk
21. [Device-GigabitEthernet0/0/2] port trunk pvid vlan 30
22. [Device-GigabitEthernet0/0/2] port trunk allow-pass vlan 30
[Device-GigabitEthernet0/0/2] quit

23. Create device files to be deployed.
a. Choose Resource > Network > Zero Touch Provisioning > Configuration File Making from the main menu.

b. Click Create and set parameters.

c. Click Next and perform basic configuration for lower-layer devices.
If basic configuration is not performed, lower-layer devices cannot be properly added to eSight for management after they are deployed based on the topology plan.
The following basic configuration is only for reference and the configuration in the site plan prevails:

```
#
sysname $NEname
#
vlan $vlan
#
lldp enable
#
interface Vlanif $vlan
ip address dhcp-alloc
#
interface $interface_type_in $interface_number_in
port link-type trunk
port default vlan $vlan
#
interface $interface_type_out1 $interface_number_out1
port link-type trunk
port default vlan $vlan
#
interface $interface_type_out2 $interface_number_out2
port link-type trunk
port default vlan $vlan
#
ip route-static 10.137.58.0 255.255.0.0 10.137.58.1
#
user-interface maximum-vty 5
user-interface vty 0 4
authentication-mode password
user privilege level 15
set authentication password cipher $password
protocol inbound telnet
#
return
```

After configuring related basic configuration commands, click Refresh Template Parameters, set related template variables based on the plan, and click OK.

d. Repeat the preceding substeps to create configuration files of other devices.
e. (Optional) Prepare software, patches, and license files of devices to be deployed based on the site requirements.
Choose Resource > Network > Configuration > Device Software Management from the main menu. Choose File Management from the navigation tree on the left and upload the correspon
24. Create a deployment task.
a. Choose Resource > Network > Zero Touch Provisioning > Topo Plan-based Provisioning from the main menu.

b. Right-click a blank area and select Create Task.

c. Set Root type to campus and Task name to Task for Department AB, and select Auto Active.

d. Click OK.

25. Plan the network topology through topology deployment.
a. Plan the network topology through topology deployment. Double-click the deployment task and click Add Root Device.

b. Select the root device.

c. On the Plan Topology tab page, right-click a root device, choose Add Remote Device > Switches from the shortcut menu, set related parameters, and click OK to add an aggregation dev

d. Click OK.

e. Add an access device of department A. In detail, right-click the aggregation device S5701, choose Add Remote Device > Switches from the shortcut menu, set related parameters, and c

f. Add an access device of department B. In detail, right-click the aggregation device S5702, choose Add Remote Device > Switches from the shortcut menu, set related parameters, and c

g. Adjust the topology and save it. The sorted root device, aggregation device, and access devices are displayed.

h. (Optional) If device information needs to be modified, right-click the corresponding device and choose Modify from the shortcut menu.

26. Match device files for the devices to be deployed.
a. Click the Match File tab, right-click the aggregation device, and choose Match Provisioning File from the shortcut menu. On the page that is displayed, select the corresponding deployme
OK.

b. Repeat the preceding substeps to match device files of other devices.

27. Clean up configurations for the devices to be deployed and restart the devices

To ensure that device configurations are empty, you are advised to perform the configuration cleanup operation.
Run the following command to clean up the device configurations:

```
reset saved-configuration
y
```

delete /unreserved *.cfg
y
delete /unreserved *.zip
y
reboot
n //Select n here. Otherwise, the device generates a new configuration file.
y
The devices to be deployed are assigned with temporary IP addresses through the DHCP server, enter the topology plan-based deployment process, and send deployment requests.
28. Compare topologies.
eSight collects the network topology of the deployment area from the root device, compares the network topology with the planned topology, and displays the differences for users to corre
a. Click the Compare Topologies tab, right-click the root device, and choose Manually Topology Collection from the shortcut menu.

If the comparison fails, click Configure Cluster Management VLAN, verify the configuration of the cluster management VLAN, and perform configuration based on the plan again.
b. Confirm the comparison result.
If the comparison result indicates that the topology is incorrect, check and correct the physical connections.
29. Trigger and start the deployment based on the topology plan.
a. Click the Start Provisioning tab, right-click all devices to be deployed, and choose Start to provision.
b. (Optional) Activate devices.
If automatic activation is not selected during deployment task creation, you need to manually activate the devices.
The devices must be activated from bottom to top one by one based on the topology. An upper-layer device can be activated only when the lower-layer device is activated and restarted su
upper-layer device is activated first, lower-layer devices are disconnected from the network after the upper-layer device restarts. As a result, the topology plan-based deployment fails.
c. Verify that the deployment status is displayed as successful for each device, indicating that the topology plan-based deployment is complete.
Result
Choose Topology > Topology Management from the main menu after the deployment is completed. All deployed devices can be displayed, and alarm messages of the devices can be report

Diante do exposto fica claro que o sistema de gerência eSight não só possui a funcionalidade de ZTP (Zero Touch Provisioning) como atende integralmente o item 25.10.1.10.
A Recorrente se perde na análise da proposta e documentações, e aparenta não deter os mínimos conhecimentos técnicos para a devida apreciação dos documentos, ressalte-se, muito pelos técnicos da FUNASA.

Destaca-se que o pregoeiro agiu com total zelo e detalhada análise à documentação da habilitação técnica apresentada por esta Recorrida, proferindo sua certa e adequada decisão.

Após apresentar as provas acima, não nos resta dúvida que a recorrente tem um único propósito com esse descabido recurso apresentado que é justamente atrasar a compra dessa Admir

Dessa forma, não há qualquer razão para alterar a decisão já tomada, acertadamente, pela Pregoeira e que respeita todos os princípios basilares dos certames licitatórios.

A inabilitação da vencedora sob os argumentos apresentados, como requer a recorrente, além de significar total afronta ao princípio da obtenção da proposta mais vantajosa, visto apresentou o menor preço, e a diferença entre a recorrente (segundo lugar no ranking das melhores propostas) é de R$ 812.000,00,, significaria conduta viciada por excesso de formal vista que todos os requisitos do Edital e da Lei foram cumpridos pela recorrida.

Aliás, a decisão desta Nobre Pregoeira obedece a orientação do TCU esculpida no acórdão 357/2015-Plenário:

"No curso do procedimento licitatório, a Administração Pública deve pautar-se pelo princípio do formalismo moderado, que prescreve a adoção de formas simples e suficientes para pro grau de certeza, segurança e respeito aos direitos dos administradores, promovendo, assim, a prevalência do conteúdo sobre o formalismo externo, respeitada, ainda, as praxes essenciais prerrogativas dos administrados."

Nesta mesma vertente de entendimentos do TCU de que:

"Ao constatar incertezas sobre o cumprimento de disposições legais ou editalicias, especialmente dúvidas que envolvam critérios e atestados que objetivam comprovar a habilitação da disputa, o responsável pela condução do certame deve promover diligências para aclarar os fatos e confirmar o conteúdo dos documentos que servirão de base para a tomada Administração (Art. 43, § 3° da Lei 8666/93) ." (Acórdão TCU n°. 3.418/2014 – Plenário).

Portanto, é nítido que a Nobre Pregoeira em nenhum momento se distanciou das regras estabelecidas no edital e seus anexos os quais respeitam a legislação vigente e o entendime Superiores, já que todos os cuidados foram tomados por esta para garantir a segurança jurídica, a isonomia e a razoabilidade na condução deste certame para declarar vencedora a vantajosa e que atendeu a todos os requisitos estabelecidos no edital, a da recorrida.

Contudo, mesmo diante dos erros cometidos pela recorrente em suas razões recursais e visando não deixar dúvidas ao julgador do processo licitatório de que foi observado o princípio d instrumento convocatório e declarada vencedora a proposta mais vantajosa para o item, todos os itens questionados a respeito ao objeto ofertado pela recorrida foram respondidos, confo acima já expostos, e podem ser comprovados pela documentação oficial já encaminhada ao Ministério do Turismo através do parecer técnico emitido após diligências.

III. DO PEDIDO:

Diante do exposto, a Recorrida DESDE JÁ REQUER seja dado total improcedência ao pedido e seja julgado improvido o recurso interposto pela recorrente – NTSEC SOLUCÕES EM TELEINFO - no que diz respeito ao mérito recursal, mantendo-se, na íntegra, a decisão que declara vencedora do Grupo 01 a recorrida, e realizando-se a adjudicação e homologação do item proposta comercial e documentação técnica atenderam a todos os requisitos do instrumento convocatório sem trazer nenhum prejuízo à Fundação Nacional de Saúde – FUNASA e se mos menor preço e mais vantajosa nos ditames do instrumento convocatório.

Termos em que, pede deferimento.

Palhoça, 20/07/2020.

ZOOM TECNOLOGIA LTDA
CNPJ 06.105.781/0001-65

OBS: Por conter figuras a contrarrazão será enviada para o e-mail cpl@funasa.gov.br aos cuidados de Adalberto Caetano Lopes.

Fechar