GOVERNO DO ESTADO DE MINAS GERAIS

SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTÃO

Ata de Audiência Pública - Diretoria Central de Gestão de Serviços e Infraestrutura de TIC - Secretaria de Estado de Planejamento e Gestão

O Estado de Minas Gerais por meio da Diretoria Central de Gestão de Serviços e Infraestrutura de TIC e da Central de Compras, situada na Secretaria de Estado de Planejamento e Gestão, e também por meio da Diretoria de Infraestrutura Tecnológica, situada na Secretaria de Estado de Educação, realizou de forma virtual a Audiência Pública do Registro de Preços para aquisição de equipamentos de infraestrutura de rede lógica para o provimento de conectividade WiFi no dia 30 de setembro de 2022 às 10:00.

O Termo de Referência proposto e as documentações complementares foram disponibilizadas no Portal de Compras de Minas Gerais, site www.compras.mg.gov.br; os interessados foram encorajados a manifestar-se previamente à realização da audiência, encaminhando suas dúvidas e considerações até o dia 28 de setembro de 2022 via e-mail. A publicação também ocorreu no Diário do Executivo no dia 16/09/2022 na pág. 67. (55730099)

Isto posto, segue as ponderações realizadas:

AGILITA Consultoria e Desenvolvimento de Negócios (Paulo Andrade Junior ME)

Sobre o item 7.14: Não serão aceitos atestados/certificados que apresentem informações divergentes entre o item do certificado/atestado e o apresentado na proposta, exceto nos casos em que forem apresentadas declarações das próprias entidades certificadoras comprovando que as diferentes nomenclaturas correspondem aos mesmos modelos ofertados, não sendo aceitos documentos do próprio licitante, sob pena de desclassificação da proposta apresentada.

Pergunta: Qual o entendimento exato sobre os "mesmos modelos ofertados"?

Resposta: A documentação apresentada deverá corresponder ao modelo ofertado, não podendo haver divergência.

Entendemos que equipamentos similares ao modelo ofertado estarão em acordo com a exigência da Lei nº. 8666/93, Artº 30, § 3º, ou seja, equipamentos que possuam funcionalidades semelhantes, apenas com diferenças de capacidades de alcance e quantidade de dispositivos conectados, por exemplo, mas com similaridade nos processos de importação, distribuição e instalação, entre outros, no nosso entender, representam o atendimento da exigência para a capacidade técnica e operacional garantindo assim, a correta execução do contrato.

Por outro lado, se considerarmos o estrito termo "modelo", os equipamentos do atestado a ser apresentado ficariam limitados em séries e códigos de fabricantes iguais aos da proposta, com apenas evolução da versão, o que tornaria a participação restritiva, indo contra o princípio da ampla concorrência.

Outrossim, já há precedentes no mercado de recursos julgados nesta linha, com entendimento, uma vez que a linha de equipamentos é ampla e diversificada em muitas vertentes de mercado, todavia sujeita-se aos mesmos processos de fornecimento.

Resposta: Mesmo se tratando de mudanças de série e códigos do fabricante deve haver um novo atestado do equipamento.

ALTAS NETWORKS & TELECOM

PONTO DE ACESSO INTERNO

1. LICENCIAMENTO E GERENCIAMENTO:

1) Solicita a inclusão do subitem:

Sugestão: "Deve possuir garantia de fábrica do tipo Limited Life time, contemplando 5 anos de substituição de equipamentos defeituosos após o fabricante anunciar o encerramento do ciclo de vendas do produto ofertado;"

Resposta: A sugestão de inclusão não será acatada.

---

2. HARDWARE

2) Texto Original: Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (devendo ser utilizado cabo de segurança com chave ou similar);

Sugestão de alteração: Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (devendo ser utilizado cabo de segurança com chave ou similar); Deverá ser fornecido com Kensington ou similar;

Resposta: A sugestão de inclusão não será acatada.

---

4. SEGURANÇA

3) Texto Original: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 e SAE-AES;

Sugestão de alteração: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES;

Resposta: A sugestão será atendida parcialmente:

"Poderá ser implementado WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES ou, ainda, implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal."

---

5. RÁDIO

4) Texto Original: Deve Suportar no mínimo 512 clientes por rádio (1024 por AP)

Sugestão de alteração: Deve Suportar no mínimo 256 clientes por rádio (512 por AP)

Resposta: A especificação será readequada:

"Deve Suportar no mínimo 256 clientes por rádio (512 por AP)"

---

6. INFORMAÇÕES COMPLEMENTARES

5) Texto Original: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem.

Sugestão de alteração: Deve possuir suporte a captive portal web (HTTPS) de autenticação do tipo splash page externo para operar em conjunto com a solução de autenticação centralizada.

Resposta: A especificação será readequada:

"Deve possuir suporte a captive portal web (HTTPS) de autenticação do tipo splash page externo para operar em conjunto com a solução de autenticação centralizada."

---

6) Texto Original: Deve incluir solução de controladora em nuvem responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários.

A solução de Controladora Wireless em Nuvem deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração.

Sugestão de alteração: 9.8.1.Para pontos de acesso que não suportem operar em modo auto gerenciado, devem ser fornecidos com controladoras virtuais ou físicas, em redundância, instalado em infraestrutura da contratada permitindo: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários. Toda a

comunicação entre controladoras e access points deverá ser criptografada.

Para soluções virtualizadas, deverão fazer parte do fornecimento os servidores necessários, obedecendo às especificações mínimas recomendadas pelo fabricante para a volumetria de access points, assim como sistemas operacionais e software complementares para a completa instalação do sistema, atendendo a todas as características solicitadas.

As controladoras deverão estar licenciadas, caso necessário, para quantidade total de Pontos de Acessos descritos neste Termo de Referência e serem gerenciadas pelo item de Software de Gerenciamento deste edital.

Resposta: A sugestão não será acatada.

---

7) Texto Original: Deve implementar recursos que permitam mecanismo de autenticação através de portal Web customizável (captive portal customizável) para clientes visitantes, com usuário e senha.

Deve suportar autenticação de usuários na rede por meio de contas da Google.

Sugestão de alteração:

Deve implementar recursos que permitam mecanismo de autenticação através de portal Web customizável (captive portal customizável) para clientes visitantes, com usuário e senha, através da solução de autenticação.

O captive portal externo deve suportar autenticação de usuários na rede por meio de contas da Google.

Resposta: A sugestão não será acatada.

ITEM 2 – PONTO DE ACESSO EXTERNO

1. LICENCIAMENTO E GERENCIAMENTO:

1) Solicita a inclusão do subitem:

"Deve possuir garantia de fábrica do tipo Limited Life time, contemplando 5 anos de substituição de equipamentos defeituosos após o fabricante anunciar o encerramento do ciclo de vendas do produto ofertado;"

Resposta: A sugestão de inclusão não será acatada.

---

2. HARDWARE

2) Texto Original: Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (devendo ser utilizado cabo de segurança com chave ou similar);

Capacidade de temperatura de operação de no mínimo 50°C.

Sugestão: Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (devendo ser utilizado cabo de segurança com chave ou similar). Deverá ser fornecido com Kensington ou similar. Capacidade de temperatura de operação de no mínimo 55°C.

Resposta: A sugestão de inclusão não será acatada.

---

4. SEGURANÇA

3) Texto Original: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 e SAE-AES;

Sugestão de inclusão: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES;

Resposta: A sugestão será atendida parcialmente:

"Poderá ser implementado WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES ou, ainda, implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal."

---

5. RÁDIO

4) Texto Original: Possuir antenas internas com ganho mínimo de 2,5dBi em 2,4GHz e 3 dBi em 5GHz;

Deve suportar potência máxima de transmissão de no mínimo 17.5 dBm na frequência 2.4 GHz e de no mínimo 17.5 dBm na frequência 5 GHz;

Sugestão de alteração: Possuir antenas internas com ganho mínimo de 3

dBi em 2,4GHz e 5 dBi em 5GHz;

Deve suportar potência máxima de transmissão de no mínimo 20 dBm na frequência 2.4 GHz e de no mínimo 20 dBm na frequência 5 GHz;

Resposta: A sugestão não será acatada.

---

6. INFORMAÇÕES COMPLEMENTARES

5) Texto Original: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem.

Sugestão de inclusão: Deve possuir suporte a captive portal web (HTTPS) de autenticação do tipo splash page externo para operar em conjunto com a solução de autenticação centralizada.

Resposta: A sugestão será acatada.

---

6) Texto Original: Deve incluir solução de controladora em nuvem responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários. A solução de Controladora Wireless em Nuvem deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração.

Sugestão de alteração: 9.8.1.Para pontos de acesso que não suportem operar em modo auto gerenciado, devem ser fornecidos com controladoras virtuais ou físicas, em redundância, instalado em infraestrutura da contratada permitindo: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência),funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários. Toda a comunicação entre controladoras e access points deverá ser criptografada.

Para soluções virtualizadas, deverão fazer parte do fornecimento os servidores necessários, obedecendo às especificações mínimas recomendadas pelo fabricante para a volumetria de access points, assim como sistemas operacionais e software complementares para a completa instalação do sistema, atendendo a todas as características solicitadas.

As controladoras deverão estar licenciadas, caso necessário, para quantidade total de Pontos de Acessos descritos neste Termo de Referência e serem gerenciadas pelo item de Software de Gerenciamento deste edital.

Resposta: A sugestão não será acatada.

---

7) Texto Original: Deve implementar recursos que permitam mecanismo de autenticação através de portal Web customizável (captive portal customizável) para clientes visitantes, com usuário e senha.

Deve suportar autenticação de usuários na rede por meio de contas da Google.

Sugestão de alteração: Deve implementar recursos que permitam mecanismo de autenticação através de portal Web customizável (captive portal customizável) para clientes visitantes, com usuário e senha, através da solução de autenticação.

O captive portal externo deve suportar autenticação de usuários na rede por meio de contas da Google.

Resposta: A sugestão não será acatada.

ITEM 3 – SWITCHES

Texto Original: Temperatura de operação: 0 – 40°C;

Sugestão de alteração: Temperatura de operação: 0 – 45°C

Resposta: A sugestão não será acatada.

---

2) Solicita a inclusão do subitem: Deve possuir garantia de fábrica do tipo

Limited Life time, contemplando 5 anos de substituição de equipamentos defeituosos após o fabricante anunciar o encerramento do ciclo de vendas do produto ofertado;

Resposta: A sugestão não será acatada.

---

3) Solicita a inclusão dos subitens:

2. CARACTERÍSTICAS LÓGICAS

2.1. Deve ser do gerenciado pela mesma solução de gerenciamento dos Access Points.

2.2. Deve permitir o gerenciamento local através de interface gráfica Web no padrão HTTPS e via CLI via SSHv2

2.3. Deve suportar o padrão 802.1Q com até 512 VLANs simultâneas;

2.4. Deve suportar prevenção de loops através dos protocolos de SpanningTree STP, RSTP, MSTP e RPVST+;

2.5. Deve implementar proteções no SpanningTree de root guard;

2.6. Deve suportar DHCP snooping;

2.7. Deve suportar ACL's e QoS em IPv4 e IPv6;

2.8. Deve suportar 200 ACL's em IPv4 e 100 ACL's em IPv6;

2.9. Deve suportar padrão 802.3ad LACP suportando 8 grupos de agregações com no mínimo 3 portas em cada;

2.10. Deve suportar espelhamento de porta para entrada e saída de tráfego, com no mínimo 4 grupos;

2.11. Deve suportar duas imagens de software em flash, como primária e backup;

2.12. Deve suportar armazenamento de múltiplos arquivos de configurações a flash;

2.13. Deve suportar SNMP v1, v2c e v3

Resposta: sugestão de inclusão não será acatada.

ITEM 4 – SOLUÇÃO DE GERENCIAMENTO (ITEM 9.7 TR)

1) Texto Original: 9.7.4. A solução deve suportar e estar licenciado para gerenciar todos os APs E switches constantes neste termo de referência;

Sugestão: A solução deve suportar e estar licenciado para gerenciar todos os pontos de acesso e switches constantes neste termo de referência;

Resposta: A sugestão não será acatada.

---

2) Texto Original: 9.7.10. Prover organização hierárquica de equipamentos, permitindo que um equipamento receba as configurações lógicas e as replique a outros equipamentos;

Sugestão de alteração: Prover organização de equipamentos através de grupos, permitindo que todos equipamentos de um grupo recebam as mesmas configurações lógicas;

Resposta: A sugestão não será acatada.

ITEM 5 – AUTENTICAÇÃO (ITEM 9.8 TR)

1) Texto Original: 9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance, sendo compatível com os seguintes Hypervisors:

Sugestão de alteração: A solução de autenticação de usuários e dispositivos para controle de acesso à rede deverá ser baseada em appliance físico ou Virtual Appliance, sendo compatível com os seguintes Hypervisors:

Resposta: A especificação será adequada:

"9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance. Deverão ser providos quantos softwares e ou appliance forem necessários para realizar as funções de gerenciamento e controle de todos os pontos de acesso e switches contratados, incluindo sistema operacional e todas licenças necessárias."

---

2) Texto Original: 9.8.5. Possuir plataforma unificada que combina AAA, NAC, BYOD e acesso de convidado incorporando identidade, integridade,

informações físicas/ de dispositivo e elementos condicionais em um conjunto de políticas

Sugestão de alteração: Possuir plataforma unificada que combinadamente suporte AAA e acesso de convidado incorporando identidade, integridade, informações físicas/ de dispositivo e elementos condicionais em um conjunto de políticas.

Resposta: A especificação será readequada:
"9.8.5 Possuir plataforma unificada que combina AAA e controle de acesso de usuários convidados."

---

3) Texto Original:

9.8.13. Deve possuir Dashboard customizável, onde deve permitir a visualização de no mínimo as seguintes informações:

9.8.13.1. Lista com os últimos Alertas do sistema;

9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authentication;

9.8.13.3. Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 dias;

9.8.14. Para soluções compostas por mais de um servidor/appliance, deve apresentar o Status de cada elemento dos sistemas, com informações como endereço IP e data da última replicação dos dados.

9.8.14.1. Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação.

9.8.14.2. Últimas falhas de autenticação;

9.8.14.3. Lista com as últimas autenticações

9.8.14.4. Lista com as últimas autenticação com sucesso

9.8.15. Utilização de CPU do sistema, no mínimo nos últimos 30 minutos;

Sugestão de alteração:

Deve possuir Dashboard customizável, onde deve permitir a visualização de no mínimo as seguintes informações:

Lista com os últimos Alertas do sistema;

Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authentication;

Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 dias;

Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação.

Últimas falhas de autenticação;

Lista com as últimas autenticações

Lista com as últimas autenticação com sucesso

Utilização de CPU do sistema, no mínimo nos últimos 30 minutos;

Resposta: A especificação será readequada

O texto do item 9.8.14 será removido, porém seus subitens serão mantidos.

9.8.13.1. Lista com os últimos Alertas do sistema;

9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ ou similar e Web Authentication;

9.8.13.3. Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 dias;

9.8.13.4. Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação.

9.8.13.5. Últimas falhas de autenticação;

9.8.13.6. Lista com as últimas autenticações

9.8.13.7. Lista com as últimas autenticação com sucesso

9.8.15. Utilização de CPU do sistema, no mínimo nos últimos 30 minutos;

---

4) Texto Original: 9.8.21. Deve implementar os serviços de autenticação, profiling e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos.

Sugestão de alteração: Deve implementar os serviços de autenticação e profiling para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos.

Resposta: A sugestão não será acatada

---

5) Texto Original: 9.8.26. Deve suportar a verificação de vulnerabilidade através de varredura de portas (NMAP).

Sugestão de alteração: Deve suportar profiling de devices através de varredura de portas utilizando NMAP.

Resposta: A sugestão não será acatada.

FIBERX

Item 1: Quais serão os quantitativos para cada item solicitado?

- Ponto de acesso interno

- Ponto de acesso externo

- Switch

- Rack

- Nobreak

- Serviço de instalação

- Treinamento

Resposta: Será incluído no Termo de Referência - ANEXO D - PORTE E QUANTIDADES

Item 1.2.2.1: Sabemos que existem unidades em locais tombados pelo patrimônio público. Como será o processo de autorização para intervenção nestes locais, caso seja necessário alterações que poderão ser consideradas em não conformidade com a legislação específica e qual é o quantitativo destas unidades?

Resposta: Os locais tombados pelo patrimônio público serão indicados, bem como as informações necessárias para realização das obras nesses locais.

Item 2.2: Esta é uma contratação de grande porte e há descrição específica e justificativas sensatas e legais quanto a não participação de ME e EPP. Aproveitando este tema perguntamos: qual será o capital social mínimo exigido?

Resposta: O Edital possuirá cláusulas que tratarão da Qualificação Financeira, que seguem a padronização adotada pela Administração Pública Estadual:

11.9.1. Certidão negativa de falência expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida pelo distribuidor do domicílio da pessoa física, emitida nos últimos 06 (seis) meses;

11.9.2. Balanço Patrimonial e demonstrações contábeis do último exercício, já exigíveis e apresentados na forma da lei, que deverão ser apresentados por todos os licitantes independentemente do tipo de empresa, vedada a sua substituição por balancetes ou balanços provisórios, comprovando que a licitante possui boa situação financeira, avaliada pelos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC).

11.9.2.1. Serão aceitos como na forma da Lei o Balanço Patrimonial e demonstrações contábeis assim apresentados:

11.9.2.1.1. Sociedades regidas pela Lei Federal nº 6.404/76 (Sociedade Anônima):

11.9.2.1.1.1. Publicadas em Diário Oficial; ou

11.9.2.1.1.2. Publicados em jornal; ou

11.9.2.1.1.3. Por cópia registrada ou autenticada na Junta Comercial da sede ou domicílio do licitante;

11.9.2.1.2. Sociedades Limitadas (LTDA):

11.9.2.1.2.1. Por cópia do Livro Diário, devidamente autenticado na Junta Comercial da sede ou domicílio do licitante ou em outro órgão equivalente, inclusive com os Termos de Abertura e de Encerramento; ou

11.9.2.1.2.2. Por cópia do Balanço e das Demonstrações Contábeis devidamente registrados ou autenticados na Junta Comercial da sede ou do domicílio do licitante;

11.9.2.1.3. Sociedades sujeitas ao regime estabelecido na Lei Complementar Federal nº 123/06 (Lei das Microempresas e das Empresas de Pequeno Porte) – "SIMPLES NACIONAL":

11.9.2.1.3.1. Por cópia do Balanço e das Demonstrações Contábeis devidamente registrados ou autenticados na Junta Comercial da sede ou do domicílio do licitante;

11.9.2.2. Os documentos exigidos neste subitem, quando forem próprios,

deverão ser assinados pelo representante legal do licitante e pelo seu contador ou, quando publicados em Órgão de Imprensa Oficial, deverão permitir a identificação do veículo e da data de sua publicação e conter o nome do contador e o número de seu registro no Conselho Regional de Contabilidade.

11.9.3. As pessoas jurídicas obrigadas a adotar a Escrituração Contábil Digital– ECD, bem como as sociedades empresárias que facultativamente aderiram ao sistema, nos termos da Instrução Normativa da Receita Federal do Brasil nº 1.774, de 22 de dezembro de 2017, poderão apresentar a ECD para os fins previstos no item 10.9.2 do edital.

11.9.4. No caso de empresa constituída há menos de 1 (um) ano, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período da existência da sociedade.

11.9.5. A composição da boa situação financeira da empresa será verificada por meio do cálculo do índice contábil da empresa a ser entregue, considerando-se habilitadas as licitantes que apresentarem os Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), maiores ou iguais a 1 (um) extraídos das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

11.9.6. Nas situações que as empresas licitantes não atinjam, em um dos índices mencionados no ITEM 10.9.5, valor maior ou igual ao valor do índice previsto no edital, poderá comprovar de forma alternativa, a existência de patrimônio líquido correspondente a, no mínimo, até 10% do valor estimado da contratação.

11.9.6.1. Para fins do cumprimento do item 10.9.6 o valor estimado da contratação será considerado equivalente ao valor total da proposta do fornecedor.

Item 6: Dado a complexidade e dimensão do projeto acreditamos ser importante a exigência de parceiro oficial do fabricante e que deva possua um número mínimo de profissionais qualificados pelo fabricante compatível com a envergadura deste projeto.

Pergunta: Quais serão estas exigências em termos de quantitativos de profissionais certificados pelo fabricante?

Resposta: A informação será incluída no Termo de referência

9.5.1.11. A CONTRATANTE deverá possuir pelo 01 (um) profissional certificado pelo fabricante dos equipamentos e soluções

---

Item 6.2: Podem definir com mais detalhes o que seriam “compatíveis” para os casos de atestados de capacidade técnica apresentados em somatório? Por exemplo: atestados citando equipamentos para comunicação e transmissão de dados, voz e imagens usando protocolo IP serão considerados compatíveis?

Resposta: Está correto o entendimento.

Item 9.5.1.4: Entendendo que o prazo proposto é realmente curto, haverá possibilidade de trabalhos de instalação e comissionamento aos finais de semana e em feriados? - para atender o cronograma informado, qual a expectativa da SEE relativa a quantidade de equipes simultâneas trabalhando nas localidades?

Resposta: As instalações e comissionamentos devem ser realizados de segunda à sexta, no horário de funcionamento das escolas.

Item 9.3: Sabendo que os equipamentos constantes nesse termo de referência são uma união de itens de hardware, software e serviços, há o entendimento de que os mesmos poderão ser faturados respeitando as devidas diferenças de discriminação do item e alíquotas tributárias, ou seja, a garantia e licenciamento do equipamento “ponto de acesso” deverá ser faturada como Nota Fiscal de Serviços e ter seus devidos tributos pagos, já para o item de hardware do equipamento, haverá incidência de ICMS. Está correto o entendimento?

Resposta: O entendimento não está correto. A garantia e o licenciamento são características inerentes à aquisição dos equipamentos.

Item 9.7.7.: A solução deve estar instalada em infraestrutura da CONTRATADA podendo ser migrado para infraestrutura da CONTRATANTE no término do contrato ou quando for solicitado.

Pergunta: Será permitido utilizar uma infraestrutura de terceiros? Ou seja, ser instalado em infraestrutura sob responsabilidade da contratada?

Resposta: Vide todo item 16.2. "DA SUBCONTRATAÇÃO", no termo de referência

"16.2. Por tais razões, considerando ser a parte menor e de pouca relevância frente ao valor total do certame, a subcontratação somente será admitida para os serviços de instalação."

Item 9.7.17.: Deve possuir informação visual e gráfica, planta baixa dos andares, para:

9.7.17.1. Visualização dos APs instalados, com estado de funcionamento;

9.7.17.2. Visualização do mapa de calor de RF (Heatmap);

9.7.17.3. Localização de ativos conectados à rede (equipamentos 802.11);

9.7.17.4. Localização de rogue Aps;

9.7.17.5. Caso esta funcionalidade não esteja disponível no sistema de gerência, deve ser fornecido software, do mesmo fabricante, para atender este item.

Pergunta: Será fornecida a planta dos andares e das demais escolas? Em qual formato? O site survey poderá ser preditivo ou somente presencial?

Resposta: Não serão fornecidas plantas arquitetônicas. Não haverá projeto de site survey. As instalações serão realizadas em locais pré definidos.

Item 9.7.30.2. Informações sobre chamadas de voz, seus protocolos e qualidade das mesmas. Estas características não são de um escopo de gerenciamento WIFI, além disso, chamadas de voz podem ter influências externas, quais protocolos e níveis de qualidade se esperam medir? O texto é muito genérico.

Resposta: O texto será removido

Item 9.7.31. Deve possuir informação sobre possíveis ameaças à rede detectadas pelos sistemas gerenciados;

9.7.32. Deve possibilitar criação de regras de detecção de ameaças e correlacionar todos os dispositivos gerenciados.

Pergunta: Busca-se uma solução de gerenciamento WIFI ou uma solução de gerenciamento de

Segurança? Estas são características de SIEM que fogem do escopo e os itens devem ser suprimidos.

Resposta: O texto será removido

Item 9.8.1.: Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance, sendo compatível com os seguintes Hypervisors:

9.8.1.1. VmWare ESXi 5.5 ou superior;

9.8.3. A solução deve ser disponibilizada em infraestrutura da CONTRATADA, devendo ser transferida para infraestrutura da CONTRATANTE ao fim do contrato ou quando for solicitado.

Pergunta: Quais os critérios de autenticação de alunos, professores e colaboradores para ser autenticado? Qual a base de dados consultar? Existe uma padronização? A base é única ou múltiplas bases?

Resposta: A autenticação será via e-mail Google.
A especificação será alterada:

9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance. Deverão ser providos quantos softwares e ou appliance forem necessários para realizar as funções de gerenciamento e controle de todos os pontos de acesso e switches contratados, incluindo sistema operacional e todas licenças necessárias.

Item

9.8.8.1. Multifator de autenticação OnConnect

9.8.9. Recursos do 360 Security Exchange, incluindo servidores de contexto de endpoint locais e ações de servidor de contexto para o host local e XML.

Respostas: Para o item 9.8.8.1. A especificação será readequada:
"9.8.8.1. Multifator de autenticação"

Resposta: Para o item 9.8.9. A especificação será readequada:

"A solução de autenticação deve permitir integração com ferramentas de segurança de terceiros, tipo antivírus, firewall."

Item 9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authentication;

Pergunta: Solução de autenticação Cisco, aceita similar?

Resposta: A especificação será readequada.

"9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ ou similar e Web Authentication;"

Item 9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting;

Pergunta: Solução de fabricante Cisco, será aceito similar?

Resposta: Serão aceitas soluções similares.

Item 9.8.25.11. TACACS+ Pergunta: Solução de fabricante Cisco, será aceito similar?

Resposta: A especificação será readequada.

"9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ ou similar e Web Authentication;"

Item 9.8.28.

Permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informações a serem utilizadas durante o processo de autenticação dos usuários.

Pergunta: Serão aceitas outras bases de dados?

Resposta: No processo de autenticação, deverão ser usadas as bases de dados definidas pelo órgão.

Item 15.1. e (Item 9.7.17): Este item dispõe sobre a não necessidade da vistoria técnica. Neste caso perguntamos se haverá possibilidade de execução remota do site survey para aquelas unidades que possuírem planta em formato DWG ou PDF com medidas. Se positivo, qual seria o quantitativo destas unidades?

Resposta: Não serão fornecidas plantas arquitetônicas. Não haverá projeto de site survey. As instalações serão realizadas em locais pré definidos.

Referente ao Anexo A - ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS/SEE/DITE/2022, ITENS 1 e 2

6. INFORMAÇÕES COMPLEMENTARES

Deve incluir solução de controladora em nuvem responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários.

Pergunta: A solução de gerenciamento exige funções de segurança de um escopo de firewall e devem ser suprimidas.

Resposta: A sugestão não será acatada

ITEM 3 – SWITCH

Favor confirmar o item: Jumbo Frame: 10 Kb

Pergunta: Este tamanho não é usual em switches de acesso, será revisado o item?

Resposta: A sugestão será acatada, será alterado para 9KB

ITEM 5 - NOBREAK

Pergunta: Qual o tempo esperado de autonomia em carga plena?

Resposta: Deve prover autonomia prevista em manual

Pergunta: Quais equipamentos serão suportados pelo nobreak?

Resposta: Os equipamentos que compõem a solução wi-fi

Pergunta: Ficará dentro ou fora do rack?

Resposta: Poderá ficar fora da rack

Item 9.8.21.: Deve implementar os serviços de autenticação, profiling e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos.

Pergunta: Este número seria de usuários simultâneos? Caso não, qual seria a quantidade de usuários/dispositivos simultâneos?

Resposta: A quantidade informada é de usuários simultâneos.

ITEM 4 - RACKS

Pergunta: A profundidade solicitada é de 50 cm, entendemos que é uma profundidade mínima, sendo aceita modelos padrão de mercado com profundidade de 55 cm?

Resposta: Sim. Esta profundidade pode ser aceita

No item também especifica o peso máximo de 13 Kg para o rack considerando a capacidade de instalação máxima, entretanto este é quase o peso de um rack com estas características sem equipamentos. Assim, entendemos que o peso de 13 Kg deve ser o peso máximo não considerando equipamentos. Está correto o nosso entendimento?

Resposta: O valor de peso informado se refere ao peso do rack vazio.

NO ITEM 6 - SERVIÇO DE INSTALAÇÃO

No item não menciona a necessidade de certificação do cabeamento, assim, entendemos que não será necessário a certificação dos pontos de rede deste projeto. Está correto o entendimento?

Resposta: O entendimento está correto.

BETTA

Comentário: Na intenção de colaborarmos com o Processo de contratação de "Equipamentos WiFi", solicitamos que nos esclareçam as seguintes dúvidas:

1. Qual a quantidade de AP's internos por escola?

2. Qual a quantidade de AP's externos por escola?

3. Qual a quantidade de Switches ?

4. Qual a quantidade de nobreaks?

5. Qual a quantidade de Racks?

Resposta: Será incluído no Termo de Referência - ANEXO D - PORTE E QUANTIDADES

Pergunta: A solução de autenticação deverá ser obrigatoriamente instalada em ambiente disponibilizado pela contratada? Ou pode ser no ambiente da contratante?

Resposta: Deverá ser, obrigatoriamente, instalada em ambiente disponibilizado pela contratada.

Pergunta: As fontes de autenticação deverão ser todas suportadas? Ou somente algumas?

9.8.6. Suporte a seguintes fontes para autenticação:

9.8.6.1. Microsoft Active Directory

9.8.6.2. Kerberos

9.8.6.3. LDAP-compliant directory

9.8.6.4. ODBC-compliant SQL server

9.8.6.5. Token servers

9.8.6.6. Base SQL interna

9.8.6.7. Radius

9.8.6.8. Microsoft Azure Active Directory

9.8.6.9. Google G Suite

9.8.6.10. HTTP

9.8.6.11. Lista estática de endereços MAC

Resposta: A especificação será readequada:

Para o item 9.8.6 e seus subitens serão consideradas as especificações a seguir:

9.8.6. Suporte a seguintes fontes para autenticação:

9.8.6.1. Microsoft Active Directory

9.8.6.2. LDAP

9.8.6.3. Base SQL interna

9.8.6.4. Radius

9.8.6.5. Google G Suite

9.8.6.6. HTTP

9.8.6.7. Lista estática de endereços MAC autenticação

OI SOLUÇÕES

QUESTIONAMENTO 1

Quanto ao que descreve o item 1.2.8: "1.2.8. Os ativos de rede (ponto de acesso, switches, nobreak) devem vir com etiqueta de patrimônio conforme modelo e range a ser fornecido pela SEE."

Entendemos que a etiqueta de patrimônio será fornecida pela SEE. Nosso entendimento está correto?

Resposta: O entendimento não está correto, a SEE fornecerá somente o modelo e range.

QUESTIONAMENTO 2

Quanto ao que descreve o item 3.4: "Quanto ao quantitativo estimado, registre-se a relação das escolas e suas características como fator principal na definição da volumetria do projeto. Tal detalhamento está explicitado na Planilha do ANEXO B - LOCAIS DE ENTREGA e INSTALAÇÃO (52854259)"

Entendemos que será fornecido a planta dos locais onde os equipamentos serão instalados, bem como o local onde o mesmo será conectado ao link de internet de forma que a Contratada possa formatar uma proposta mais coerente com necessidade do Contratante. Nosso entendimento está correto?

Resposta: O entendimento não está correto. Não serão fornecidas plantas. A localização será pré-definida de acordo com os ambientes de cada localidade.

QUESTIONAMENTO 3

Quanto ao que descreve o item 9.1: Prazo de Entrega:

9.1.1. Os equipamentos adquiridos deverão ser entregues em até 90 (noventa) dias corridos contados do dia seguinte ao recebimento da. Nota de Empenho, Autorização de Fornecimento ou documento equivalente."

Devido ao atual contexto de escassez da cadeia global de semicondutores para a produção de chips e componentes eletrônicos, ocasionados pelas restrições impostas pela pandemia de COVID-19, agravada pelo recente conflito entre Rússia e Ucrânia e também com o fechamento de Portos estratégicos para a logística mundial advindas por uma nova onda da COVID-19 na Ásia, e considerando que tais elementos são utilizados como matéria prima para a montagem de equipamentos de rede. Devido a isso sugerimos uma flexibilização no prazo de entrega para pelo menos 120 dias e caso seja necessária será permitida e extensão do prazo de entrega citado, desde que seja apresentado um pedido formal da contratada, devidamente embasado por documentação oficial do fabricante, informando os motivos do atraso e ações a serem tomadas para acelerar o processo e novas datas de entrega propostas. Nossa solicitação será aceita?

Resposta: Os prazos deverão ser cumpridos de acordo com o cronograma (ANEXO B - LOCAIS DE ENTREGA E INSTALAÇÃO) que será readequado.

QUESTIONAMENTO 4

Quanto ao que descreve o item 9.5.1.3: "9.5.1.3. A infraestrutura elétrica e cabeada será de responsabilidade da Contratada, incluindo os patches cords de manobra para instalação do AP que devem ser fornecidos pela Contratada;"

Entendemos que será fornecido as plantas dos sites de onde deverão ser ativados os APs, bem como do local de onde será buscado a saída para internet. Nosso entendimento está correto?

Resposta: O entendimento não está correto. Não serão fornecidas plantas. A localização será pré-definida de acordo com os ambientes de cada localidade.

QUESTIONAMENTO 5

Quanto ao que descreve o item 11.2:

"11.2. O contrato tem vigência por 36 meses, a partir da publicação de seu extrato no Diário Oficial do Estado de Minas Gerais."

Entendemos que o objeto será fornecido como serviço e não aquisição por uma vigência de 36 meses. Nosso entendimento está correto?

Resposta: O entendimento não está correto. O fornecimento como serviço corresponde apenas a instalação e treinamento.

QUESTIONAMENTO 6

Quanto às especificações do item subitem 3, Conexão e Rede, do Item 2, Ponto de acesso Externo, do Anexo A Especificações Técnicas dos Equipamentos / SEE / DITE / 2022

"Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior e uma interface 1G SFP;"

Com o intuito de se favorecer a competitividade no certame, permitindo uma equalização de preços entre os fabricantes participantes da licitação, solicitamos à SEE que a interface SFP 1G seja fornecida em caráter opcional ou que sejam permitidas alternativamente interfaces elétricas multigigabit (100/1000/2500BASE-T) e MDI/MDX. Nossa sugestão será aceita?

Resposta: A sugestão não será aceita.

QUESTIONAMENTO 7

Quanto às especificações do item 3, SWITCHES, do Anexo A Especificações Técnicas dos Equipamentos / SEE /DITE /2022 "Jumbo Frame: 10KB;"

À fim de que a competitividade no certame seja favorecida, permitindo a participação de importantes fabricantes de equipamentos de redes, solicitamos à SEE que a capacidade de Jumbo Frames mínima seja de 9198 (nove mil cento e noventa e oito) bytes. Nossa sugestão será aceita?

Resposta: Será alterado para 9 Kb.

QUESTIONAMENTO 8

Quanto ao que descrevem os itens 9.7.1, 9.7.7, 9.7.8:

“9.7.1. Os equipamentos devem incluir Solução de Gerência da Rede Sem Fio deve ser fornecida em Appliance Virtual;”

“9.7.7. A solução deve estar instalada em infraestrutura da CONTRATADA podendo ser migrado para infraestrutura da CONTRATANTE no término do contrato ou quando for solicitado.

“9.7.8. A solução deverá ser disponibilizada através da imagem de sistema operacional, já com os softwares necessários para a instalação em VMWARE.”

Quanto às especificações do subitem 6, Informações Complementares, do Item 1, Ponto de acesso Interno, e do Item 2, Ponto de acesso Externo, do Anexo A Especificações Técnicas dos Equipamentos / SEE / DITE / 2022.

“Deverá ser fornecida e instalada a versão mais recente do software interno do ponto de acesso WiFi.”

“Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem.”

O Termo de Referência específica no item 9.7 que deverá ser provido uma solução de gerenciamento dos APs no formato de virtual appliance. Entendemos que esta gerência em VM deverá ser fornecida também as licenças de controladora em nuvem para os APs Indoor e Outdoor.

Nosso entendimento está correto?

Resposta: O entendimento está correto.

QUESTIONAMENTO 9

Entendemos que a Contratada não realizará intervenção na configuração de equipamentos e/ou links de terceiros. Nosso entendimento está correto?

Resposta: O entendimento está correto.

QUESTIONAMENTO 10

Entendemos que a Contratada não se responsabilizará pelo atendimento remoto para abertura de chamados externos (conexões WAN de terceiros), ou seja, a Contratada não terá qualquer responsabilidade por equipamentos e/ou links de terceiros. Nosso entendimento está correto?

Resposta: O entendimento está correto.

QUESTIONAMENTO 11

Entendemos que a Contratada não comunicará o cliente caso ocorram quedas e ou degradação dos links de terceiros. Nosso entendimento está correto?

Resposta: O entendimento está correto.

QUESTIONAMENTO 12

Entendemos que no momento da instalação pela Contratada do equipamento, os links de terceiros contratados pelo cliente deverão estar ativos e suas conexões disponíveis para que a Contratada possa realizar as interligações com os equipamentos providos pela Contratada. Nosso entendimento está correto?

Resposta: O entendimento está correto.

QUESTIONAMENTO 13

Entendemos que no momento da instalação pela Contratada do equipamento, os links de terceiros contratados pelo cliente deverão estar ativos e suas conexões disponíveis para que a Contratada possa realizar as interligações com os equipamentos fornecidos pela contratada. Nosso entendimento está correto?

Resposta: O entendimento está correto.

QUESTIONAMENTO 14

Entendemos que a Contratada deixa o Contratante ciente que em casos de quedas e/ou degradação dos links de terceiros, o gerenciamento do

equipamento provido pela Oi sofrerá impacto e a Contratada não poderá ser penalizada em caso de perda de cumprimento de SLA por problemas causados por terceiros.

Nosso entendimento está correto?

Resposta: O entendimento está correto.

QUESTIONAMENTO 15

DA VEDAÇÃO DE PARTICIPAÇÃO DE LICITANTES EM REGIME DE CONSÓRCIO

O item 5.1 do Termo de Referência veda a participação de empresas que estejam constituídas em consórcio.

Tal determinação fulmina diretamente a competitividade do certame por não existir grande número de empresas qualificadas para prestação do serviço licitado e pela própria complexidade do objeto licitado. Ademais, verifica-se que o próprio artigo 33 da Lei n.º 8666/93 permite expressamente a participação de empresas em consórcio.

Assim, quanto às particularidades do mercado de telecomunicações, pode-se afirmar que as restrições de participação de empresas nas licitações devem ser, mais que em outros casos, motivadas. Isto porque, em homenagem aos princípios da competitividade e isonomia, apenas se podem admitir as restrições objetivas e legítimas.

Ante o exposto, de forma a possibilitar a participação de um maior número de empresas no certame, garantindo a sua competitividade e a busca pela proposta mais vantajosa à Administração Pública requer alteração do item 5.1 do Termo de referência para que seja permitida a participação em consórcio de empresas, nos termos do art. 33 da Lei n.º 8.666/93 e no art. 15 da Lei nº 14.133/2021.

Resposta: A sugestão não será aceita.

QUESTIONAMENTO 16

REAJUSTE

Os serviços telefônicos podem ser remunerados por meio da cobrança de tarifas ou de preços. A remuneração acontecerá pela cobrança de tarifas quando o serviço telefônico for prestado em regime público, por meio de Concessão. Por sua vez, a cobrança pelos serviços de telecomunicações prestados em regime privado acontecerá por meio de preços.

Ocorre que considerando o objeto do edital tratar-se de SCM, e sua remuneração ser feita por preços e não tarifas, torna-se imperioso que o índice de reajuste dos preços relativos a sua prestação de serviço, seja o IGP-DI

Ante o exposto, requer a adequação do item 11.3 do Termo de Referência, de modo que o reajuste dos preços seja realizado não pelo IPCA, mas sim pelo IGP-DI:

"A Contratada poderá reajustar os preços de cobrança dos serviços a cada 12 meses, a contar da data de assinatura do presente instrumento, considerando seu valor básico atualizado até esta data, devendo ser utilizado como índice de reajuste o IGP-DI".

Resposta: A sugestão não será aceita. O item mencionado segue o disposto na Resolução Conjunta SEPLAG/SEF nº 8.898/2013.

QUESTIONAMENTO 17

DA GARANTIA DE EXECUÇÃO

O item 14.1.1 do termo de referência estabelece a exigência de apresentação de garantia de 5% do valor do contrato.

Como se sabe, a atividade administrativa exige prestígio aos princípios da razoabilidade e proporcionalidade.

Desta feita, a apresentação de garantia no percentual exigido não é razoável, razão pela qual se requer a modificação do item supracitado, para que a garantia exigida corresponda ao limite máximo de 3% (quatro por cento).

Resposta: A sugestão não será aceita.

QUESTIONAMENTO 18

DAS PENALIDADES EXCESSIVAS

O item 18.1.2.2 do termo de referência determina a aplicação de multas que extrapolam o limite de 10% (dez por cento) sobre o valor do contrato estabelecido pelo Decreto n.º 22.626/33, em vigor conforme Decreto de 29 de novembro de 1991, pois traz 20% de multa sobre o valor do objeto

A fixação de multa nesse patamar também ofende a Medida Provisória n.º 2.172/01 (e suas reedições), aplicável a todas as modalidades de contratação, inclusive aquelas firmadas entre particulares e Administração Pública.

Por todo o exposto, requer a adequação do item 18.1.2.2 do termo de referência para que as multas aplicadas observem o limite de 10% (dez por cento)

Resposta: As multas previstas na seção Sanções Administrativas são padrão dos Editais da Administração Pública Estadual. A sugestão não será aceita.

QINTESS

SERVIÇO DE INSTALAÇÃO (ITEM 9.5)

Texto Original: 9.5.1.3. A infraestrutura elétrica e cabeada será de responsabilidade da Contratada, incluindo os patches cords de manobra para instalação do AP que devem ser fornecidos pela Contratada;

Comentário: Entendemos que referente a infraestrutura elétrica que necessária em cada escola será composta por Resposta: 1 (um) ponto de energia 110VAC ou 220VAC que será utilizado para alimentar o nobreak onde será conectado os ativos de rede (AP´s e switch), e nos casos em que ponto de energia existente estiver longe do local de acomodação do rack dos equipamentos a contratada será responsável por estender o cabeamento de energia até este rack. Nosso entendimento está correto?

Resposta: O entendimento está correto. Por padrão, o local onde será instalado o rack já está provido de ponto elétrico. Caso seja necessário a mudança de dimensionamento das tomadas para utilização do nobreak somente a troca da tomada para o padrão 20A já será o suficiente para instalação.

SOLUÇÃO DE GERENCIAMENTO (ITEM 9.7)

Texto Original: 9.7.10. Prover organização hierárquica de equipamentos, permitindo que um equipamento receba as configurações lógicas e as replique a outros equipamentos;

Comentários: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Prover organização hierárquica de equipamentos, permitindo que a configuração seja feita no grupo de equipamentos de forma que todos os equipamentos que fazem parte desse grupo irá receber essa configuração.

Resposta: A sugestão não será acatada.

Texto Original: 9.7.14. Permitir a visualização de eventuais áreas sem cobertura de RF (áreas de sombra);

Comentários: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Sugerimos a retirada deste item pois a funcionalidade já é atendida através do item 9.7.17.2 Visualização do mapa de calor de RF (Heatmap);

Resposta: A sugestão não será acatada.

Texto Original: 9.7.29. Possibilitar a identificação de paredes e divisórias com respectivos níveis de atenuação por tipo (alvenaria, vidro, drywall e divisória);

Comentários: Solicitamos a retirada deste item para evitar assim, a participação de um único fabricante no processo licitatório.

Resposta: A sugestão não será acatada.

Texto Original: 9.7.30.2. Informações sobre chamadas de voz, seus protocolos e qualidade das mesmas;

Comentários: Solicitamos a retirada deste item para evitar assim, a participação de um único fabricante no processo licitatório.

Resposta: O texto será removido.

Texto Original: 9.7.31. Deve possuir informação sobre possíveis ameaças à rede detectadas pelos sistemas gerenciados;

Comentários: Solicitamos a retirada deste item para evitar assim, a participação de um único fabricante no processo licitatório.

Resposta: O texto será removido.

Texto Original: 9.7.32. Deve possibilitar criação de regras de detecção de ameaças e correlacionar todos os dispositivos gerenciados.

Comentários: Solicitamos a retirada deste item para evitar assim, a participação de um único fabricante no processo licitatório.

Resposta: O texto será removido.

Texto Original: 9.7.33.3. Deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos.

Comentários: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Deve ser disponibilizado endereço de e-mail ou portal de suporte para abertura dos chamados técnicos.

Resposta: A sugestão será acatada.

Texto Original:

9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance, sendo compatível com os seguintes Hypervisors:

9.8.1.3. Amazon EC2;

9.8.1.4. CentOS KVM;

Comentários: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance, sendo compatível no mínimo com os seguintes Hypervisors:

9.8.1.3. Amazon EC2;

Comentários: Solicitamos a retirada deste item para evitar assim, a participação de um único fabricante no processo licitatório.

9.8.1.4. CentOS KVM;

Comentários: Solicitamos a retirada deste item para evitar assim, a participação de um único fabricante no processo licitatório.

Resposta: A especificação será readequada

9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance. Deverão ser providos quantos softwares e ou appliance forem necessários para realizar as funções de gerenciamento e controle de todos os pontos de acesso e switches contratados, incluindo sistema operacional e todas as licenças necessárias.

Texto Original: 9.8.5 até 9.8.34 (incluindo subitens)

9.8.5. Possuir plataforma unificada que combina AAA, NAC, BYOD e acesso de convidado incorporando identidade, integridade, informações físicas/ de dispositivo e elementos condicionais em um conjunto de políticas.

9.8.6. Suporte a seguintes fontes para autenticação:

9.8.6.1. Microsoft Active Directory

9.8.6.2. Kerberos

9.8.6.3. LDAP-compliant directory

9.8.6.4. ODBC-compliant SQL server

9.8.6.5. Token servers

9.8.6.6. Base SQL interna

9.8.6.7. Radius

9.8.6.8. Microsoft Azure Active Directory

9.8.6.9. Google G Suite

9.8.6.10. HTTP

9.8.6.11. Lista estática de endereços MAC

9.8.7. Deve estar licenciado para as seguintes fontes para autenticação:

9.8.7.1. 802.1x

9.8.7.2. MAC

9.8.8. Registro e autenticação de usuário baseado na Web (como autor-registro, sponsor based e social-login).

9.8.8.1. Multifator de autenticação OnConnect

9.8.9. Recursos do 360 Security Exchange, incluindo servidores de contexto de endpoint locais e ações de servidor de contexto para o host local e XML.

9.8.10. Demais recursos devem ser suportados através de upgrades futuros da solução.

9.8.11. Deve suportar "Single Sign-on" (SSO) através de SAML v2.0. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

9.8.11.1. Atributos do usuário autenticado,

9.8.11.2. Hora do dia, dia da semana,

9.8.11.3. Tipo de dispositivo utilizado,

9.8.11.4. Localização do usuário;

9.8.11.5. Tipo de autenticação utilizado

9.8.12. Permitir a visualização de todas as informações relativas a cada transação/autenticação em uma única tela, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise.

9.8.13. Deve possuir Dashboard customizável, onde deve permitir a visualização de no mínimo as seguintes informações:

9.8.13.1. Lista com os últimos Alertas do sistema;

9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authentication;

9.8.13.3. Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 dias;

9.8.14. Para soluções compostas por mais de um servidor/appliance, deve apresentar o Status de cada elemento dos sistemas, com informações como endereço IP e data da última replicação dos dados.

9.8.14.1. Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação.

9.8.14.2. Últimas falhas de autenticação;

9.8.14.3. Lista com as últimas autenticações

9.8.14.4. Lista com as últimas autenticações com sucesso

9.8.15. Utilização de CPU do sistema, no mínimo nos últimos 30 minutos;

9.8.16. Deve implementar funcionalidade de classificação automática de dispositivos (“Device profiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;

9.8.17. Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.), por sistema operacional (ex. Windows, Linux, MacOS, etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server, etc);

9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting;

9.8.29.3. IPv6 Accounting Proxy;

9.8.29.4. Acesso a servidores com endereçamento IPv6 para contexto de endpoints;

9.8.29.5. Syslog, DNS, NTP;

9.8.29.6. Endereçamento IPv6 para VIP (Virtual IP) de alta disponibilidade;

9.8.29.7. Fontes de Syslog para processamento de evento

9.8.29.8. Validações e conformidades:

9.8.29.8.1. FIPS 140-2

9.8.29.8.2. Common Criteria NDcPP + Servidor de autenticação

9.8.30. A solução deve permitir configuração em alta disponibilidade com no mínimo dois elementos, sendo que ambos devem permanecer ativos para o processamento das requisições;

9.8.31. A solução deve permitir a configuração centralizada de políticas em ambientes distribuídos, no qual as políticas serão configuradas em um único elemento para serem distribuídas aos demais que pertençam à mesma "zona"

9.8.32. A solução deve permitir a geração e o envio através de email ou SMS de alertas relativos às seguintes atividades anormais detectadas na rede:

9.8.32.1. Autenticações

9.8.32.2. Acesso a dispositivos de rede

9.8.32.3. Tentativa de execução de comandos em dispositivos de rede por usuários sem privilégios

9.8.32.4. Atividades irregulares nos servidores da solução.

9.8.33. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML e PDF.

9.8.34. A solução deve ter suporte do fabricante no horário das 08:00h às 20:00h de segunda a sexta feira, durante todo o período de contrato.

9.8.29.3. IPv6 Accounting Proxy;

Solicitamos a retirada destes itens para evitar assim, a participação de um único fabricante no processo licitatório. Propomos o descritivo abaixo do item 9.8.5 até 9.8.32 para atender os requisitos com maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra:

9.8.5. Possuir plataforma unificada que combina AAA e controle de acesso de usuários convidados.

9.8.6. Deve vir licenciado para permitir o cadastramento de, no mínimo, 25.000 (vinte e cinco mil) usuários simultâneos

9.8.7. A solução deve suportar clusterização no modo ativo/ativo ou ativo/passivo para prover resiliência e alta disponibilidade.

9.8.8. Permitir a criação de páginas personalizadas para o captive portal, com a inclusão de imagens, instruções em texto e campos de texto que possam ser preenchidos pelos clientes;

9.8.9. Deve suportar autenticação de usuários através de redes sociais suportando, no mínimo, integração com Facebook, LinkedIn e Google.

9.8.10. Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo visitante e em caso de autosserviço, especificando quais informações cadastrais dos visitantes são requisitadas.

9.8.11. Deve exigir que o usuário visitante aceite o “Termo de uso da rede” a cada login ou apenas no primeiro login.

9.8.12. Deve implementar um portal web seguro (HTTPS) a ser apresentado automaticamente aos usuários temporários durante o início de sua conexão com a rede.

9.8.13. Deve implementar o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), e-mail ou impressão local.

9.8.14. O portal de autenticação deve ser suportado, no mínimo, pelos seguintes navegadores de Internet: Microsoft Internet Explorer, Mozilla Firefox, Safari e Chrome, operando em PCs e dispositivos móveis.

9.8.15. Permitir a automatização do processo de conexão segura à rede sem fio através da instalação automática de certificado digital e configuração de perfil de rede sem fio em dispositivos móveis

9.8.16. A solução deve provisionar automaticamente um certificado digital para o dispositivo cadastrado e configurar o dispositivo com o certificado gerado e com as configurações de rede sem fio para que o usuário utilize autenticação segura via 802.1X na rede corporativa

9.8.17. A solução deve identificar automaticamente o tipo de dispositivo cadastrado e conectado à rede para provisionar o certificado digital e configurar o perfil da rede sem fio conforme o sistema operacional utilizado e deverá suportar, no mínimo, os seguintes sistemas operacionais: Apple iOS, Windows, Mac OSx e Android

9.8.18. A solução deve guiar/instruir o usuário durante o procedimento de instalação do certificado digital e configuração do perfil da rede sem fio através de página web ou através de aplicativo

9.8.19. Após a finalização do processo de autosserviço e configuração do suplicante, a solução deve desconectar o dispositivo do usuário da rede visitante (captive portal) e conectá-lo automaticamente na rede corporativa com autenticação 802.1X em dispositivos que suportem tal ação

9.8.20. A solução deve instalar os certificados digitais através de CA (Certification Authority) interna na ferramenta (certificado digital auto assinado) ou também permitir a utilização de certificados digitais de CA externas (Root CA do Active Directory, por exemplo)

9.8.21. A solução deverá integrar diretamente ou através de servidor RADIUS com o Active Directory da Microsoft para identificação e autenticação dos usuários

9.8.22. Deve suportar a autenticação PEAP por meio de servidor RADIUS embarcado, diretamente em contato com a base de dados de usuários sem a necessidade de servidor RADIUS externo ou terceiro

9.8.23. Possuir capacidade de autenticação dos usuários visitantes através de senhas pré-cadastradas ou vouchers, para cada usuário ou grupo de usuários, no caso de utilização em eventos

9.8.24. Permitir a configuração do número máximo de conexões simultâneas realizadas por uma mesma conta, possibilitando que um usuário possua mais de um dispositivo na rede com a mesma senha e que contas coletivas sejam utilizadas em eventos. Esta funcionalidade deve ser aplicada para usuários visitantes autenticados

pelo captive portal

9.8.25. Deve oferecer visibilidade e controle sobre dispositivos na rede com a possibilidade de revogar o acesso

9.8.26. Realizar verificação de postura dos dispositivos quando os mesmos se associam pela primeira vez, incluindo checagem de antivírus, configurações de registro, patches, proxy, firewall, entre outros, com a possibilidade de remediação

9.8.27. Deve suportar OCSP (Online Certificate Status Protocol) com revogação automática

9.8.28. Deve suportar integração com OAuth 2.0 e SAML 2.0 para autenticação externa

9.8.29. Deve prover REST APIs para permitir integração com soluções de terceiros

9.8.30. Deve suportar Radius CoA (Change of Authorization) para o servidor RADIUS interno

9.8.31. Disponibilizar servidor SMTP interno ou possibilitar a configuração de servidor SMTP externo para envio de e-mails

9.8.32. Deve ser possível solicitar ao usuário visitante, no passo de autenticação, a inserção do e-mail da pessoa responsável por aprovar o seu acesso à rede, sendo que essa pessoa se encarregará por aprovar ou rejeitar a requisição uma vez que o sistema a notifique

RESPOSTA: As especificações serão readequadas ou acatadas parcialmente, conforme elencadas a seguir:

- **9.8.5. Possuir plataforma unificada que combina AAA e controle de acesso de usuários convidados.**
- **Para o item 9.8.6 e seus subitens serão consideradas as especificações a seguir:**
- **9.8.6. Suporte a seguintes fontes para autenticação:**
  - **9.8.6.1. Microsoft Active Directory**
  - **9.8.6.2. LDAP**
  - **9.8.6.3. Base SQL interna**
  - **9.8.6.4. Radius**
  - **9.8.6.5. Google G Suite**
  - **9.8.6.6. HTTP**
  - **9.8.6.7. Lista estática de endereços MAC autenticação**

- **Para o item 9.8.8 e seus subitens serão consideradas as especificações a seguir:**
- **9.8.8. Registro e autenticação de usuário baseado na Web, por meio de auto-registro ou login através de rede social.**
  - **9.8.8.1. Multifator de autenticação**

- **9.8.9. A solução de autenticação deve permitir integração com ferramentas de segurança de terceiros, tipo antivírus, firewall**
- **9.8.12. Permitir a visualização de todas informações relativas a cada transação/autenticação, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise.**
- **9.8.14. O texto do item 9.8.14 será removido, porém seus subitens serão mantidos.**
- **9.8.16. Deve suportar expansão de licenciamento para implementar funcionalidade de classificação automática de dispositivos, de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;**
- **9.8.17. Deve suportar expansão de licenciamento para categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.), por sistema operacional.**
- **9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, SNMP e base de assinaturas;**

- **Para o item 9.8.29 e seus subitens serão consideradas as especificações a seguir:**
- **9.8.29. Suporte a servidores de autenticação e autorização com endereçamento IPv6.**
  - **9.8.29.1. Fontes de Syslog para processamento de evento**
- **9.8.30. Caso a CONTRATADA esteja ofertando solução de**

gerenciamento que não possua os recursos de autenticação do item 9.8. A mesma poderá ofertar solução integrada, de terceiros, apresentando comprovação de integração entre as soluções de gerenciamento e autenticação.

- **9.8.33. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML ou CSV ou EXCEL e PDF.**

ITEM 1 - PONTO DE ACESSO INTERNO

Texto Original: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 e SAE-AES;

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CCM-256 e SAE-AES;

Resposta: A especificação será readequada:

"Poderá ser implementado WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES ou, ainda, implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal."

Texto Original: Possuir antenas internas com ganho mínimo de 2,5dBi em 2,4GHz e 3 dBi em 5GHz;

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Possuir antenas internas com ganho mínimo de 1,5dBi em 2,4GHz e 2,5 dBi em 5GHz;

Resposta: A sugestão não será acatada. No entanto, a especificação será readequada:

"Possuir antenas internas com ganho mínimo de 2dBi em 2,4GHz e 3dBi em 5GHz;"

---

6. INFORMAÇÕES COMPLEMENTARES

Texto Original: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem.

Comentário: Sugestão de alteração visando a aderência ao próprio Termo de Referência Item 6.7 SOLUÇÃO DE GERENCIAMENTO: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em Appliance Virtual.

Resposta: A especificação será readequada:

"Deve possuir suporte a captive portal web (HTTPS) de autenticação do tipo splash page externo para operar em conjunto com a solução de autenticação centralizada."

Texto Original: Deve incluir solução de controladora em nuvem responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários

Comentário: Sugestão de alteração visando a aderência ao próprio Termo de Referência Item 6.7 SOLUÇÃO DE GERENCIAMENTO: Deve incluir solução de controladora em Appliance Virtual responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários

Resposta: A sugestão será acatada parcialmente:

"Deve incluir solução de controladora em nuvem e/ou em appliance virtual instalada na infraestrutura da contratada, responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste

anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários”

Texto Original: A solução de Controladora Wireless em Nuvem deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração

Comentário: Sugestão de alteração visando a aderência ao próprio Termo de Referência Item 6.7 SOLUÇÃO DE GERENCIAMENTO: A solução de Controladora Wireless em Appliance Virtual deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração ou através de uma console master para gerenciar as soluções de gerência de rede/controladora.

Resposta: A sugestão será acatada parcialmente:

“A solução de Controladora Wireless em nuvem e/ou em appliance virtual instalada na infraestrutura da contratada, deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração”

Texto Original: Deve disponibilizar uma Console de Gerenciamento Web acessível através de protocolo Criptografado, compatível com os principais browsers do mercado (Internet Explorer, Firefox e Chrome), permitindo também acesso a Console através de dispositivos móveis com sistema operacional iOS e Android;

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Deve disponibilizar uma Console de Gerenciamento Web acessível através de protocolo Criptografado, compatível com os principais browsers do mercado (Internet Explorer, Firefox e Chrome)

Resposta: A sugestão será acatada:
“Deve disponibilizar uma Console de Gerenciamento Web acessível através de protocolo Criptografado, compatível com os principais browsers do mercado (Microsoft Edge, Firefox e Chrome)”

Texto Original: Deve permitir a criação de contas de usuários para acesso a rede WiFi. Estes usuários devem ficar armazenados na própria solução de controladora Wireless em nuvem.

Comentário: Sugestão de alteração visando a aderência ao próprio Termo de Referência Item 9.7 SOLUÇÃO DE GERENCIAMENTO: Deve permitir a criação de contas de usuários para acesso a rede WiFi. Estes usuários devem ficar armazenados na própria solução de controladora Wireless em Appliance Virtual.

Resposta: A sugestão será acatada parcialmente:

“Deve permitir a criação de contas de usuários para acesso a rede WiFi. Estes usuários devem ficar armazenados na própria solução de controladora Wireless nuvem e/ou em appliance virtual instalada na infraestrutura da contratada.”

ITEM 2 - PONTO DE ACESSO EXTERNO

Texto Original: Capacidade de temperatura de operação de no mínimo 50°C;

Comentário: Sugestão de alteração visando maior robustez e a prevenção de possíveis falhas intermitentes por aumento de temperatura ambiente, pois o patamar de 50 graus Celsius de temperatura mínima, é um patamar baixo para o Access Point externo. Capacidade de temperatura de operação de no mínimo 65°C.

Resposta: A sugestão não será acatada.

Texto Original: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 e SAE-AES;

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra:

Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CCM-256 e SAE-AES;

Resposta: A sugestão será atendida parcialmente:

“Poderá ser implementado WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES ou, ainda, implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal.”

Texto Original: Possuir antenas internas com ganho mínimo de 2,5dBi em 2,4GHz e 3 dBi em 5GHz;

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Possuir antenas internas com ganho mínimo de 2 dBi em 2,4 GHz e 3 dBi em 5GHz;

Resposta: A sugestão não será acatada.

Texto Original: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem.

Comentário: Sugestão de alteração visando a aderência ao próprio Termo de Referência Item 9.7 SOLUÇÃO DE GERENCIAMENTO: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em Appliance Virtual.

Resposta: A especificação será readequada:

“Deve possuir suporte a captive portal web (HTTPS) de autenticação do tipo splash page externo para operar em conjunto com a solução de autenticação centralizada.”

Texto Original: Deve incluir solução de controladora em nuvem responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários

Comentário: Sugestão de alteração visando a aderência ao próprio Termo de Referência Item 9.7 SOLUÇÃO DE GERENCIAMENTO: Deve incluir solução de controladora em Appliance Virtual responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários

Resposta: A sugestão será acatada parcialmente:

“Deve incluir solução de controladora em nuvem e/ou em appliance virtual instalada na infraestrutura da contratada, responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários”

Texto Original: A solução de Controladora Wireless em Nuvem deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração

Comentário: Sugestão de alteração visando a aderência ao próprio Termo de Referência Item 9.7 SOLUÇÃO DE GERENCIAMENTO: A solução de Controladora Wireless em Appliance Virtual deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração ou através de uma console master para gerenciar as soluções de gerência de rede/controladora.

Resposta: A sugestão será acatada parcialmente:

“A solução de Controladora Wireless em nuvem e/ou em appliance virtual

instalada na infraestrutura da contratada, deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração"

Texto Original: Deve disponibilizar uma Console de Gerenciamento Web acessível através de protocolo Criptografado, compatível com os principais browsers do mercado (Internet Explorer, Firefox e Chrome), permitindo também acesso a Console através de dispositivos móveis com sistema operacional iOS e Android;"

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Deve disponibilizar uma Console de Gerenciamento Web acessível através de protocolo Criptografado, compatível com os principais browsers do mercado (Internet Explorer, Firefox e Chrome)

Resposta: A sugestão será acatada:
"Deve disponibilizar uma Console de Gerenciamento Web acessível através de protocolo Criptografado, compatível com os principais browsers do mercado (Microsoft Edge, Firefox e Chrome)"

Texto Original: Deve permitir a criação de contas de usuários para acesso a rede WiFi. Estes usuários devem ficar armazenados na própria solução de controladora Wireless em nuvem.

Comentário: Sugestão de alteração visando a aderência ao próprio Termo de Referência Item 9.7 SOLUÇÃO DE GERENCIAMENTO: Deve permitir a criação de contas de usuários para acesso a rede WiFi. Estes usuários devem ficar armazenados na própria solução de controladora Wireless em Appliance Virtual.

Resposta: A sugestão será acatada parcialmente:

"Deve permitir a criação de contas de usuários para acesso a rede WiFi. Estes usuários devem ficar armazenados na própria solução de controladora Wireless nuvem e/ou em appliance virtual instalada na infraestrutura da contratada."

ITEM 5 - NOBREAKS

Texto Original: Potência de saída: 600 VA;

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Potência de saída: 600 VA ou 700VA

Resposta: A especificação será revisada.

"Potência de saída: Mínimo de 600 VA"

Texto Original: Fator de potência: 0,7;

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Fator de potência mínimo: 0,5;

Resposta: Sugestão não será acatada.

Texto Original: Forma de Onda: Senoidal;

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Forma de Onda: Senoidal ou Senoidal por aproximação (PWM);

Resposta: Sugestão não será acatada.

Texto Original: Cabo de força: Sim, com no mínimo 1,5m de comprimento;

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Cabo de força: Sim, com no mínimo 1,2m de comprimento;

Resposta: Sugestão não será acatada.

Texto Original: Atender as recomendações RoHS (Restriction of Certain Hazardous Substances)

Comentário: Solicitamos a retirada deste item para evitar assim, a participação de um único fabricante no processo licitatório.

Resposta: Sugestão não será acatada.

LOGICNET TECNOLOGIA

DO PROCESSO

Pergunta: Quanto ao atestado de capacidade técnica no valor de 10%. Este número representa a quantidade de escolas e não dos ativos que serão fornecidos, correto?

Resposta: O valor refere-se ao quantitativo mínimo de 10% (dez por cento) dos itens ofertados. Sendo admitido o somatório de atestados, desde que compatíveis com as características do objeto da licitação. Vide item 6. QUALIFICAÇÃO TÉCNICA, no Termo de Referência.

Pergunta: Visto que não tem um projeto definido a utilização de equipamento indoor e outdoor será feito definido pela secretaria, correto?

Resposta: O entendimento está correto.

Pergunta: Visto que não tem um quantitativo definido porque está excluindo o benefício da micro e pequena empresa?

Resposta: Vide item 2.2. LOTES EXCLUSIVOS PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

Pergunta: 2.2.5. Por se tratar de um ambiente descentralizado, no qual cada SRE terá a responsabilidade de gerenciar o sistema de conectividade das escolas sob sua jurisdição, a reserva de um percentual para ME/EPP afronta o princípio da razoabilidade e economicidade.

Resposta: Vide item 2.2. LOTES EXCLUSIVOS PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

Pergunta: A solução é toda em nuvem, esta justificativa não se aplica e é um descabimento. Entendemos que fere a regulamentação legal. Assim solicitamos que seja retirado este item, pois não é verdade a afirmativa acima.

Resposta: A sugestão não será acatada.

ITEM 1 - PONTO DE ACESSO INTERNO

1. LICENCIAMENTO E GERENCIAMENTO:

Texto Original: Deve ser certificado pela WIFI Alliance na subcategoria Enterprise/Service Provider Access Point, Switch/Controller or Router

Dúvida: Entendemos que cada país possui um órgão regulamentador como por exemplo a ANATEL no Brasil, portanto entendemos que serão aceitos os produtos com homologação ANATEL, além disso o produto ofertado é desenvolvido conforme normativas do IEEE, que regulamenta mundialmente os protocolos de interoperabilidade entre dispositivos wireless e cabeados garantindo assim a interoperabilidade entre equipamentos que implementam os devidos protocolos. Está correto o nosso entendimento?

Resposta: O entendimento não está correto. A certificação WIFI Alliance, na subcategoria Enterprise/Service Provider Access Point, Switch/Controller or Router pode ser requerida por qualquer fornecedor.

Texto Original: Deve possuir o certificado de Conectividade Wi-Fi CERTIFIED 6 ™ da WIFI Alliance;

Dúvida: Entendemos que cada país possui um órgão regulamentador como

por exemplo a ANATEL no Brasil, portanto entendemos que serão aceitos os produtos com homologação ANATEL, além disso o produto ofertado é desenvolvido conforme normativas do IEEE, que regulamenta mundialmente os protocolos de interoperabilidade entre dispositivos wireless e cabeados garantindo assim a interoperabilidade entre equipamentos que implementam os devidos protocolos. Está correto o nosso entendimento?

Resposta: O entendimento não está correto. O certificado de Conectividade Wi-Fi CERTIFIED 6 ™ da WIFI Alliance pode ser requerido por qualquer fornecedor.

---

2. HARDWARE

Texto Original: Deve suportar a utilização de sistema antifurto do tipo Kensington ou similar;

Dúvida: Entendemos que os Access Points de ambientação externa são alocados em locais de difícil acesso com alturas relevantes, portanto entendemos que ofertando equipamentos com os kits de instalação, atende ao ítem sem causar prejuízo ao projeto. Está correto o entendimento?

Resposta: O entendimento não está correto. Todos os equipamentos deverão suportar e deverão ser utilizados os sistemas antifurto do tipo Kensington ou similar.

Texto Original: Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (devendo ser utilizado cabo de segurança com chave ou similar);

Dúvida: Entendemos que os Access Points de ambientação externa são alocados em locais de difícil acesso com alturas relevantes, portanto entendemos que ofertando equipamentos com os kits de instalação, atende ao ítem sem causar prejuízo ao projeto. Está correto o entendimento?

Resposta: O entendimento não está correto. Todos os equipamentos deverão suportar e deverão ser utilizados os sistemas antifurto do tipo Kensington ou similar.

---

4. SEGURANÇA

Texto Original: Deve possuir rádio Bluetooth Low-Energy (BLE);

Sugestão: Retirar ítem - Não faz sentido este recurso sendo que aumenta o consumo e não tem aplicação voltada para a escola usando este tipo de dispositivo, para isso precisaria de um outro projeto já direcionado.

Resposta: A sugestão não será acatada.

Texto Original: Deve implementar recurso de Target Wake Time (TWT);

Sugestão: Retirar ítem direcionado ARUBA - https://www.arubanetworks.com/br/faq/o-que-e-wi-fi-6/

Resposta: A sugestão não será acatada. Target Wake Time (TWT) é um recurso usado em tecnologias de wi-fi 6, sendo utilizado por vários fabricantes.

---

6. INFORMAÇÕES COMPLEMENTARES

Texto Original: Deve implementar recursos de filtro de aplicação para reconhecimento e bloqueio de conteúdos relacionados a jogos, compartilhamento de arquivos, redes sociais, entre outros. Caso este recurso necessite de licença, a mesma deve ser fornecida pelo mesmo período de tempo coberto pela garantia solicitada neste termo de referência.

Sugestão: Retirar ítem - Missão de segurança deve vir do Firewall nas escolas.

Resposta: A sugestão não será acatada.

Texto Original: Deve implementar a visualização/identificação e marcação das aplicações para permitir o bloqueio ou priorização. Deve permitir a definição de endereços MAC para controle de acesso a rede WiFi.

Sugestão: Retirar ítem - Missão de segurança deve vir do Firewall nas escolas.

Resposta: A sugestão não será acatada.

Texto Original: Operador: acesso de apenas leitura às configurações para a monitoria, sem permissão para alterar configurações; Organizador de Visitantes: acesso e permissão exclusiva para criação de usuários temporários e visitantes para acesso a rede WiFi.

Sugestão: Retirar item

Resposta: A sugestão não será acatada.

Texto Original: Deve suportar autenticação de usuários na rede por meio de contas da Google.

Sugestão: Retirar item - Direcionamento

Resposta: A sugestão não será acatada.

Texto Original: Fonte de energia: 100-240 V CA, 50 / 60Hz;

Sugestão: Retirar item - Não faz mais sentido este tipo de solicitação, deve solicitar POE para os dispositivos.

Resposta: A sugestão será acatada.

ITEM 2 - PONTO DE ACESSO EXTERNO

1. LICENCIAMENTO E GERENCIAMENTO:

Texto Original: Deve ser certificado pela WIFI Alliance na subcategoria Enterprise/Service Provider Access Point, Switch/Controller or Router

Dúvida: Entendemos que cada país possui um órgão regulamentador como por exemplo a ANATEL no Brasil, portanto entendemos que serão aceitos os produtos com homologação ANATEL, além disso o produto ofertado é desenvolvido conforme normativas do IEEE, que regulamenta mundialmente os protocolos de interoperabilidade entre dispositivos wireless e cabeados garantindo assim a interoperabilidade entre equipamentos que implementam os devidos protocolos. Está correto o nosso entendimento?

Resposta: O entendimento não está correto. A certificação WIFI Alliance, na subcategoria Enterprise/Service Provider Access Point, Switch/Controller or Router pode ser requerida por qualquer fornecedor.

Texto Original: Deve possuir o certificado de Conectividade Wi-Fi CERTIFIED 6 ™ da WIFI Alliance;

Dúvida: Entendemos que cada país possui um órgão regulamentador como por exemplo a ANATEL no Brasil, portanto entendemos que serão aceitos os produtos com homologação ANATEL, além disso o produto ofertado é desenvolvido conforme normativas do IEEE, que regulamenta mundialmente os protocolos de interoperabilidade entre dispositivos wireless e cabeados garantindo assim a interoperabilidade entre equipamentos que implementam os devidos protocolos. Está correto o nosso entendimento?

Resposta: O entendimento não está correto. O certificado de Conectividade Wi-Fi CERTIFIED 6 ™ da WIFI Alliance pode ser requerido por qualquer fornecedor.

---

2. HARDWARE

Texto Original: Deve suportar a utilização de sistema antifurto do tipo Kensington ou similar;

Dúvida: Entendemos que os Access Points de ambientação externa são alocados em locais de difícil acesso com alturas relevantes, portanto entendemos que ofertando equipamentos com os kits de instalação, atende ao ítem sem causar prejuízo ao projeto. Está correto o entendimento?

Resposta: O entendimento não está correto. Todos os equipamentos deverão suportar e deverão ser utilizados os sistemas antifurto do tipo Kensington ou similar.

---

3. CONEXÃO DE REDE

Texto Original: Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior e uma interface 1G SFP; Suportar VLANs conforme o padrão IEEE 802.1Q;

Dúvida: As portas SFP e elétrica conforme o descritivo, não serão utilizadas de modo simultâneo, portanto, entendemos que poderá ser ofertado na implementação do projeto onde houver necessidade de implementação de fibra óptica a utilização de conversor de mídia, monomodo ou multimodo. Está correto o entendimento?

Resposta: O entendimento não está correto.

---

5. RÁDIO

Texto Original: Deve Suportar no mínimo 512 clientes por rádio (1024 por AP);

Sugestão: Entendemos que para a aplicação deste projeto, suportar uma capacidade de clientes acima de 250 impactará diretamente na performance dos usuários, desta forma entendemos que ofertar um Access Point com capacidade de 250 cliente por AP, atende plenamente esta solicitação. Está correto o nosso entendimento?

Resposta: A especificação será readequada:

"Deve suportar no mínimo 256 clientes por rádio (512 por AP)"

Texto Original: Deve possuir rádio Bluetooth Low-Energy (BLE);

Sugestão: Retirar ítem

Resposta: A sugestão não será acatada.

Texto Original: Deve implementar recurso de Target Wake Time (TWT);

Sugestão: Retirar item

Resposta: A sugestão não será acatada. Target Wake Time (TWT) é um recurso usado em tecnologias de wi-fi 6, sendo utilizado por vários fabricantes.

Texto Original: Deve possuir antenas direcionais.

Sugestão: Retirar item

Resposta: A sugestão não será acatada.

---

6. INFORMAÇÕES COMPLEMENTARES:

Texto Original: Deve implementar recursos de filtro de aplicação para reconhecimento e bloqueio de conteúdos relacionados a jogos, compartilhamento de arquivos, redes sociais, entre outros. Caso este recurso necessite de licença, a mesma deve ser fornecida pelo mesmo período de tempo coberto pela garantia solicitada neste termo de referência.

Sugestão: Retirar item

Resposta: A sugestão não será acatada.

Texto Original: Deve implementar a visualização/identificação e marcação das aplicações para permitir o bloqueio ou priorização. Deve permitir a definição de endereços MAC para controle de acesso a rede WiFi.

Sugestão: Retirar item

Resposta: A sugestão não será acatada.

Texto Original: Operador: acesso de apenas leitura às configurações para a monitoria, sem permissão para alterar configurações; Organizador de Visitantes: acesso e permissão exclusiva para criação de usuários temporários e visitantes para acesso a rede WiFi.

Sugestão: Retirar item

Resposta: A sugestão não será acatada.

Texto Original: Deve suportar autenticação de usuários na rede por meio de contas da Google.

Sugestão: Retirar item

Resposta: A sugestão não será acatada.

ITEM 3 - SWITCHES

Texto Original: Jumbo Frame: 10KB;

Sugestão: Entendemos que o padrão para MTBUs do tipo Jumbo frame é de 9 Kb conforme o mercado, portanto entendemos que ofertando switch com suporte de jumbo frame de 9 Kb atende ao certame. Está correto o entendimento?

Resposta: Sim, o entendimento está correto. A especificação será alterada para 9KB

Texto Original: 24 portas RJ45 10/100/1000Mbps (Auto Negociação / Auto MDI / MDIX) e 4 portas SFP 1G com fornecimento de transceiver BASESR; BASE-SR (300-400m);

Sugestão: Observação cotar os gbics

Resposta: A sugestão não será acatada.

Quanto ao que descrevem o item 9.7. SOLUÇÃO DE GERENCIAMENTO:

Texto Original	Sugestão	
9.7.14. Permitir a visualização de eventuais áreas sem cobertura de RF (áreas de sombra);	Entendemos que ofertando solução possibilitando a simulação de cobertura de acordo com a distribuição dos Aps, baseando-se em área e barreiras/interferências no qual áreas de sombra podem ser identificadas atende o item em sua totalidade. Está correto o entendimento?	Resposta: O entendimento está correto.
9.7.20.6. Suportar SSH, HTTP/HTTPS, SSL, Telnet;	O protocolo SSH (security socket shell) é um protocolo de acesso remoto criptografado, mais seguro que o telnet, e amplamente adotado por sistemas operacionais como Windows, Linux e MacOS. Portanto, entendemos que ofertando equipamento com suporte à SSH e não ao TELNET atende ao ítem em sua totalidade sem causar prejuízo ao projeto.	Resposta: O entendimento não está correto.
9.7.31. Deve possuir informação sobre possíveis ameaças à rede detectadas pelos sistemas gerenciados;	Esta capacidade relacionada a segurança da rede é mais eficiente quando implementada na rede fixa, podendo controlar o tráfego proveniente da rede cabeada e da rede sem fio. Adotando este conceito, entendemos que esta funcionalidade específica poderá ser considerada opcional e não obrigatória, visando a competição do certame. Estamos corretos em nosso entendimento?	Resposta: O entendimento está correto, o texto será removido.
9.7.32. Deve possibilitar criação de regras de detecção de ameaças e correlacionar todos os dispositivos gerenciados.		Resposta: O entendimento está correto, o texto será removido.
9.8.8.1. Multifator de autenticação OnConnect	Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf	Resposta: A especificação será readequada: "9.8.8.1. Multifator de autenticação"
9.8.9. Recursos do 360 Security Exchange, incluindo servidores de contexto de endpoint	Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba!	Resposta: A especificação será readequada: "A solução de autenticação deve

locais e ações de servidor de contexto para o host local e XML.	acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf	permitir integração com ferramentas de segurança de terceiros, tipo antivírus, firewall"
9.8.11. Deve suportar "Single Sign-on" (SSO) através de SAML	Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/techdocs/central/2.5.0/content/nms/user-mgmt/saml-profile-conf.htm	Resposta: O entendimento não está correto.
9.8.11.3. Tipo de dispositivo utilizado,	Entendemos que não faz sentido e está direcionado novamente. Assim acreditamos tirar este tipo de item.	Resposta: A sugestão não será acatada.
9.8.12. Permitir a visualização de todas informações relativas a cada transação/autenticação em uma única tela, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise.	Entendemos que disponibilizar informações de acesso do cliente conectado, porém em diferentes telas, também atende ao ítem uma vez que todas as informações solicitadas estão contidas. Tornando o certame mais competitivo trazendo maior economia ao projeto.	Resposta: A especificação será readequada: "9.8.12. Permitir a visualização de todas informações relativas a cada transação/autenticação, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise."
9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authentication;	A solução ofertada possui suporte a Radius com protocolo de autenticação. Protocolo este mais amplamente utilizado que TACACS+. Portanto entendemos que oferecendo solução com suporte a Radius, atendemos o certame na sua totalidade. Está correto o entendimento?	Resposta: A especificação será readequada: "9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ ou similar e Web Authentication;"
9.8.16. Deve implementar funcionalidade de classificação automática de dispositivos ("Device profiling"), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;	Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf	Resposta: A sugestão será acatada parcialmente e o texto será revisado. "9.8.16. Deve suportar expansão de licenciamento para implementar funcionalidade de classificação automática de dispositivos, de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;"
9.8.17. Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.), por sistema operacional (ex. Windows, Linux, MacOS, etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server, etc);	Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf	Resposta: A especificação será readequada: 9.8.17. "Deve suportar expansão de licenciamento para categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.), por sistema operacional
9.8.18. Deve suportar		Resposta: A

a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, Active Sync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting;	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	**especificação será readequada:** **"9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, SNMP e base de assinaturas;"**
9.8.21. Deve implementar os serviços de autenticação, profiling e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos.	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	**Resposta: A especificação será readequada:** **"Deve implementar os serviços de autenticação e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos, simultaneamente."**
9.8.24. Suporte a RADIUS CoA, Web authentication e SAML v2.0	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	**Resposta: A sugestão não será acatada Caso a CONTRATADA esteja ofertando solução de gerenciamento que não possua os recursos de autenticação do item 9.8. A mesma poderá ofertar solução integrada, de terceiros, apresentando comprovação de integração entre as soluções de gerenciamento e autenticação.**
9.8.25.1. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)	**?**	**Resposta: O item será removido**
9.8.25.2. PEAP (EAP-MSCHAPv2, EAP-GTC,EAP-TLS,EAP-PEAP-Public, EAP-PWD)	**?**	**Resposta: O item será mantido**
9.8.25.3. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)	**?**	**Resposta: O item será mantido**
9.8.25.4. EAP-TLS	**?**	**Resposta: O item será removido**
9.8.25.5. PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5	**?**	**Resposta: O item será removido**
9.8.25.7. SMB v2/v3	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	**Resposta: O item será removido**
9.8.25.9. RADSec	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	**Resposta: O item será removido**
9.8.25.10. Online Certificate Status Protocol (OCSP)	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	**Resposta: O item será removido**
9.8.25.11. TACACS+	**A solução ofertada possui suporte a Radius com protocolo de autenticação. Protocolo este mais amplamente utilizado que TACACS+. Portanto entendemos que oferecendo solução com suporte a Radius, atendemos o certame na sua totalidade. Está correto o entendimento?**	**Resposta: O entendimento não está correto.**
9.8.26. Deve suportar a verificação de vulnerabilidade através de varredura de portas (NMAP).	**Esta capacidade relacionada a segurança da rede é mais eficiente quando implementada na rede fixa, podendo controlar o tráfego proveniente da rede cabeada e da rede sem fio. Adotando este conceito, entendemos que esta funcionalidade específica poderá ser considerada opcional e não obrigatória, visando a competição do certame. Estamos corretos em nosso entendimento?**	**Resposta: O entendimento não está correto.**

9.8.28. Permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informações a serem utilizadas durante o processo de autenticação dos usuários.	**A solução ofertada possui suporte a Radius com protocolo de autenticação. Protocolo este mais amplamente utilizado que bases SQL. Portanto entendemos que oferecendo solução com suporte a Radius, atendemos o certame na sua totalidade. Está correto o entendimento?**	**Resposta: O entendimento não está correto.**
9.8.29. Suporte aos seguintes recursos através de IPv6:	**Todos os protocolos solicitados para ipv6 são de finalidade de gerenciamento, no qual são normalmente disponibilizados em infraestrutura interna ou serviço em nuvem. O protocolo ipv6 é amplamente adotado para a rede mundial de computadores (internet) onde não há mais endereçamentos ipv4 disponíveis, porém para redes internas em sua totalidade o protocolo ipv4 são mais amplamente adotados portanto entendendo que ofertando soluções de gerenciamento em ipv4 atende ao ítem em sua totalidade. Estamos corretos em nosso questionamento?**	**Resposta: O entendimento não está correto.** **Resposta: A especificação será readequada:** **"9.8.29. Suporte a servidores de autenticação e autorização com endereçamento IPv6;** **9.8.29.1. Fontes de Syslog para processamento de evento"**
9.8.29.1. Administração via WEB e CLI	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.2. Servidores de autenticação e autorização com endereçamento IPv6;	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.3. IPv6 Accounting Proxy;	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.4. Acesso a servidores com endereçamento IPv6 para contexto de endpoints;	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.5. Syslog, DNS, NTP;	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.6. Endereçamento IPv6 para VIP (Virtual IP) de alta disponibilidade;	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.7. Fontes de Syslog para processamento de evento	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.8. Validações e conformidades: 9.8.29.8.1. FIPS 140-2	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.8.2. Common Criteria NDcPP+Servidor de autenticação	**Entendemos que não pode haver direcionamento para fabricante, assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.30. A solução deve permitir configuração em alta disponibilidade com no mínimo dois elementos, sendo que ambos devem permanecer ativos para o processamento das requisições;	**Quando solicitado configuração em alta disponibilidade entendemos que está sendo solicitado appliance, entretanto, visando maior competitividade entendemos que ofertando solução com possibilidade de servidor virtualizado no qual possui nativamente estratégias de redundância, bem como nuvem atende ao ítem em sua totalidade sem causar prejuízo ao projeto.**	**Resposta: A sugestão não será acatada Caso a CONTRATADA esteja ofertando solução de gerenciamento que não possua os recursos de autenticação do item 9.8. A mesma poderá ofertar solução integrada, de terceiros, apresentando comprovação de integração entre as soluções de gerenciamento e autenticação.**
9.8.33. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada	**Entendemos que entregando relatórios de forma manual, atende ao ítem,**	**Resposta: O entendimento não está correto. A especificação será readequada:** **9.8.33. A solução deve possuir ferramenta**

centralizada, permitindo o agendamento e envio por e-mail em formato HTML e PDF.	tornando o certame mais competitivo trazendo maior economia ao projeto.	para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML ou CSV ou EXCEL e PDF.
9.8.34. A solução deve ter suporte do fabricante no horário de 08:00h às 20:00h de segunda a sexta feira, durante todo o período de contrato.	Entendemos que o atendimento do suporte técnico pode ser realizado por parceiros credenciados e autorizados pelo fabricante conforme horários solicitados. Está correto o entendimento?	Resposta: O entendimento está correto.

ITEM 5 - NOBREAK

Texto Original	Sugestão	
Fator de potência: 0,7;	Solicitamos que seja modificado para 0,5 permitindo assim outros participarem com indústria nacional. Essa alteração irá permitir às empresas com fabricação local o fornecimento do item aumentando assim as possibilidades de mais opções de compra.	Resposta: Não será acatado
Frequência de entrada: 50/60 HZ;	Mudar frequencia 60 HZ padrão Brasil. Essa alteração irá permitir às empresas com fabricação local o fornecimento do item aumentando assim as possibilidades de mais opções de compra.	Resposta: Não será acatado
Tipo de Tomada: mínimo 6 Tomadas/Bornes padrão NBR 14.136;	Solicitamos que seja modificado para 04, permitindo assim outros participarem com indústria nacional. Localidade que precisarem de mais tomas usa-se régua para estender, senão tudo liga no nobreak e pode comprometer. Essa alteração irá permitir às empresas com fabricação local o fornecimento do item aumentando assim as possibilidades de mais opções de compra.	Resposta: Não será acatado
Possuir porta fusível externo que acomoda uma unidade reserva;	Mudar para possuir porta fusível externo, retirar que acomode uma unidade reserva. Direcionamento. Essa alteração irá permitir às empresas com fabricação local o fornecimento do item aumentando assim as possibilidades de mais opções de compra.	Resposta: Não será acatado
Possuir a função Autoteste, pois ao ser ligado realizará os testes dos circuitos internos e das baterias;	Retirar, pois direciona, nobreak deve ter luz indicativa de uso da bateria por falta de energia. Essa alteração irá permitir às empresas com fabricação local o fornecimento do item aumentando assim as possibilidades de mais opções de compra.	Resposta: Não será acatado

Nobreak direcionado:

https://proups.com.br/produto/view/varios-modelos-station-ii-600-800-e-1200-va#.YzRcTnbMLIU

Resposta: Não foi confirmado o direcionamento para o equipamento nobreak, tendo em vista que diversos fabricantes atendem às especificações do item presente no Termo de Referência.

HUAWEI

1. CONSIDERAÇÕES GERAIS

Texto Original: 1.2.5. Todos os produtos em hardware, software e licenças de um grupo devem ser de um único fabricante, de modo a garantir plena compatibilidade.

Sugestão de Alteração: 1.2.5. Todos os produtos em hardware, software e licenças de um grupo devem ser de um único fabricante, exceto os itens 4 – Rack e 5 – Nobreak, de modo a garantir plena compatibilidade.

Justificativa: Solicitamos que os itens 4 – Rack e 5 – Nobreak possam ser de fabricantes diversos ao da solução de WLAN e LAN, já que esses itens são suplementares e não integráveis à gerência da solução principal. A Huawei comercializa no mercado brasileiro a linha de UPS (Uninterruptible Power Supply, comumente chamado de Nobreak), entretanto disponibiliza apenas equipamentos robustos para ambientes de datacenter. Diversos outros fabricantes não possuem o equipamento Nobreak em suas linhas comerciais. Os racks são comercializados pelos fabricantes, mas, assim como o Nobreak, é solicitado em característica simples e de pequeno porte, sendo a composição da solução com fabricantes especializados de Rack e Nobreak mais vantajosa financeiramente à administração pública, os quais terão equipamentos adequados para o porte solicitado, sem prejuízos ao bom funcionamento da solução de WLAN e LAN para as escolas de MG.

Resposta: A sugestão será readequada:

"1.2.5. Todos os produtos em hardware, software e licenças de um grupo devem ser de um único fabricante, exceto os itens: 3-Switch, 4-Rack e 5-Nobreak, de modo a garantir plena compatibilidade."

Adicionar: Os equipamentos sujeitos à homologação na ANATEL devem possuir certificado válido na entrega do equipamento.

Justificativa: Solicitamos adicionar (sugestão: no tópico: "7. CRITÉRIOS DE ACEITABILIDADE DA PROPOSTA")

condição para apresentação da homologação da ANATEL para todos os itens sujeitos ao processo de

homologação no momento da entrega dos equipamentos.

Resposta: A sugestão não será acatada. Pois de acordo com subitem 7.6: Serão avaliados os aspectos e padrões mínimos de aceitabilidade conforme ANEXO A - ESPECIFICAÇÕES TÉCNICAS.

Texto Original:

7.3. Caso a compatibilidade com as especificações demandadas, sobretudo quanto a padrões de qualidade e desempenho, não possa ser aferida pelos meios previstos no subitem acima, o Pregoeiro exigirá que o licitante classificado em primeiro lugar apresente amostra, sob pena de não aceitação da proposta, no local a ser indicado e dentro de 5 (cinco) dias úteis contados da solicitação.

7.7. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

Sugestão de Alteração: 7.3. Caso a compatibilidade com as especificações demandadas, sobretudo quanto a padrões de qualidade e desempenho, não possa ser aferida pelos meios previstos no subitem acima, o Pregoeiro exigirá demonstração do recurso a ser aferido dentro de 5 (cinco) dias úteis contados da solicitação. A demonstração deve ser realizada preferencialmente de forma remota, também sendo aceita demonstração com amostra local.

7.7. No caso de não haver a demonstração exigida, sem justificativa aceita pelo Pregoeiro, ou sendo constatado que a demonstração das especificações previstas neste Edital, a proposta do licitante será recusada.

Justificativa: Solicitamos que, no caso das especificações demandadas não possam ser verificadas pela documentação fornecida, seja solicitado teste remoto de forma preferencial em alternativa à entrega de amostras locais. O teste remoto assegura as condições de teste, eliminando a possibilidade do fornecedor afirmar falhas no cenário preparado pelo cliente para os testes. O teste remoto ainda pode ser realizado de forma mais célere, sem atrasos no processo para a entrega de equipamento de amostra.

Resposta: A sugestão não será acatada, pois o texto não exclui a possibilidade da demonstração ser realizada de forma remota.

---

2. CONSIDERAÇÕES TÉCNICAS

1. PONTO DE ACESSO INTERNO

Texto Original: Possuir capacidade de montagem em parede e teto, devendo ser fornecidos todos os acessórios necessários para estas montagens;

Sugestão de Alteração: Possuir capacidade de montagem em parede e teto, devendo ser fornecidos todos os acessórios necessários para estas montagens, devendo ser do mesmo fabricante do ponto de acesso.

Justificativa: Com o objetivo de assegurar total compatibilidade dos acessórios fornecidos, eliminando chances de soluções improvisadas que possam interferir no melhor funcionamento das antenas, sugerimos que os acessórios de montagem sejam obrigatoriamente do mesmo fabricante dos APs.

Resposta: A sugestão não será acatada.

Texto Original: Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c ou SNMPv3, incluindo a geração de traps;

Sugestão de Alteração: Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps, ou NETCONF.

Justificativa: A primeira parte da sugestão tem como objetivo assegurar a implementação do SNMPv3, assim como é solicitado no software de gerenciamento item "9.7.22.". O SNMPv3 fornece todas as funções do SNMPv1 e SNMPv2, e apresenta um mecanismo de segurança que autentica e criptografa pacotes SNMP. Em termos de segurança, o SNMPv3 enfatiza a segurança dos dados e o controle de acesso. O SNMPv3 garante a segurança dos pacotes SNMP das seguintes maneiras:

1. Verificação da integridade dos dados Os dados não podem ser modificados de forma não autorizada. A alteração da sequência de dados é limitada à extensão permitida.

2. Autenticação de origem de dados O SNMPv3 autentica o nó gerenciado do qual a origem é recebida e não o aplicativo que gera o pacote.

3. Confidencialidade dos dados: Quando o NMS ou o agente recebe um pacote, verificam a hora em que o pacote é gerado. Se a diferença entre a hora de criação e a hora do sistema exceder o limite, o pacote será descartado. Desta forma, os pacotes que são modificados por mal-intencionados não são aceitos.

A segunda parte da sugestão é a adição de uma alternativa de protocolo de gerenciamento. A sugestão apenas acrescenta uma alternativa, não altera para os fabricantes que implementam a gerência por meio de SNMP. O NETCONF, assim como o SNMP, é um protocolo aberto e inclusive mais interoperável que o SNMP.

O Network Configuration Protocol (NETCONF) é um protocolo de gerenciamento de rede que permite que um sistema de gerenciamento de rede (NMS) entregue, modifique e exclua configurações de dispositivos de rede.

As interfaces de programação de aplicativos (APIs) padrão estão disponíveis em dispositivos de rede para que o NMS gerencie os dispositivos usando o NETCONF. Para superar as desvantagens da CLI e do SNMP, o

NETCONF baseado em XML é introduzido, que tem as seguintes vantagens:

1. NETCONF usa uma estrutura de protocolo hierárquico, tornando-o mais adequado para requisitos de big data, automatizados e sob demanda de redes baseadas em nuvem.

2. NETCONF usa codificação XML para definir mensagens e usa o mecanismo RPC para modificar dados de configuração. Isso facilita o gerenciamento de dados de configuração e a interoperabilidade entre dispositivos de diferentes fornecedores.

3. O NETCONF realiza operações em dispositivos baseados no modelo YANG, reduzindo falhas de rede causadas por erros de configuração manual.

4. NETCONF fornece mecanismos de segurança, como autenticação e autorização para garantir a segurança da transmissão de mensagens.

5. O NETCONF fornece um mecanismo de transação para oferecer suporte à classificação, armazenamento e migração de dados, envio baseado em fases, isolamento de configuração, bem como entrega, verificação e reversão de configuração geral, minimizando o impacto nos serviços de rede.

Resposta: A sugestão será acatada parcialmente:

"Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c ou SNMPv3, incluindo a

geração de traps e/ ou NETCONF”

Texto Original: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 e SAE-AES;

Sugestão de Alteração: Implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal.

Justificativa: Solicitamos a alteração para termos utilizados pela Wi-Fi Alliance (https://www.wi-fi.org/discover-wi-fi/security) para definir os padrões de segurança WPA3. O texto sugerido possibilita a fácil compreensão e identificação ao atendimento de diversos fabricantes e engloba os modos de criptografia de 128, 192 e 256 bits.

Resposta: A sugestão será atendida parcialmente:

“Poderá ser implementado WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES ou, ainda, implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal.”

Texto Original: Possuir antenas internas com ganho mínimo de 2,5dBi em 2,4GHz e 3 dBi em 5GHz;

Sugestão de Alteração: Possuir antenas internas com ganho mínimo de 2dBi em 2,4GHz e 3 dBi em 5GHz;

Justificativa: Solicitamos alteração de ganho em 2.4GHz de 2,5 para 2 dBi. A pequena alteração não afeta no funcionamento da solução e limita a participação de fabricantes com equipamentos adequados ao porte das escolas.

Resposta: A sugestão será acatada:

Possuir antenas internas com ganho mínimo de 2dBi em 2,4GHz e 3 dBi em 5GHz;

Texto Original: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem.

Sugestão de Alteração: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem em infraestrutura privada e de uso exclusivo da Secretaria de Estado de Educação de Minas Gerais.

Justificativa: Sugestão para clarificar o modo de implementação da controladora/gerência. O texto “nuvem” pode ser interpretado como nuvem pública. Apesar de já estar descrito no software de gerenciamento que a solução deve estar instalada em infraestrutura da contratada para ser posteriormente migrada para a infraestrutura da contratante, a descrição pode ser mais clara nos APs para não restar dúvidas que não serão aceitas soluções em nuvem pública.

Resposta: A sugestão não será acatada.

Texto Original: Deve incluir solução de controladora em nuvem responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários.

Sugestão de Alteração: Deve incluir solução de controladora em nuvem em infraestrutura privada e de uso exclusivo da Secretaria de Estado de Educação de Minas Gerais responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários.

Justificativa: Sugestão para clarificar o modo de implementação da controladora/gerência. O texto “nuvem” pode ser interpretado como nuvem pública. Apesar de já estar descrito no software de gerenciamento que a solução deve estar instalada em infraestrutura da contratada para

ser posteriormente migrada para a infra-estrutura da contratante, a descrição pode ser mais clara nos APs para não restar dúvidas que não serão aceitas soluções em nuvem pública.

Resposta: A sugestão não será acatada.

Texto Original: A solução de Controladora Wireless em Nuvem deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração.

Sugestão de Alteração: A solução de Controladora Wireless em Nuvem em infraestrutura privada e de uso exclusivo da Secretaria de Estado de Educação de Minas Gerais deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de

Referência em um mesmo console de administração.

Justificativa: Sugestão para clarificar o modo de implementação da controladora/gerência. O texto "nuvem" pode ser interpretado como nuvem pública. Apesar de já estar descrito no software de gerenciamento que a solução deve estar instalada em infraestrutura da contratada para ser posteriormente migrada para a infraestrutura da contratante, a descrição pode ser mais clara nos APs para não restar dúvidas que não serão aceitas soluções em nuvem pública.

Resposta: A sugestão não será acatada.

---

2. PONTO DE ACESSO EXTERNO

Texto Original: Possuir capacidade de montagem em parede e teto, devendo ser fornecidos todos os acessórios necessários para estas montagens;

Sugestão de Alteração: Possuir capacidade de montagem em parede e teto, devendo ser fornecidos todos os acessórios necessários para estas montagens, devendo ser do mesmo fabricante do ponto de acesso.

Justificativa: Com o objetivo de assegurar total compatibilidade dos acessórios fornecidos, eliminando chances de soluções improvisadas que possam interferir no melhor funcionamento das antenas, sugerimos que os acessórios de montagem sejam obrigatoriamente do mesmo fabricante dos APs.

Resposta: A sugestão não será acatada.

Texto Original: Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior e uma interface 1G SFP;

Sugestão de Alteração: Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior e uma interface 1G SFP. Deve vir com fornecimento de 1 transceiver BASESR; BASE-SR (300-400m).

Justificativa: Sugerimos solicitar o transceiver necessário para a utilização da porta óptica do AP externo.

Resposta: A especificação será readequada.

"Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior e uma interface 1G SFP. Deve ser fornecido transceiver, caso o modelo não suporte conexão direta da fibra BASESR; BASE-SR (300-400m)."

Texto Original: Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c ou SNMPv3, incluindo a geração de traps;

Sugestão de Alteração: Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps, ou NETCONF.

Justificativa: A primeira parte da sugestão tem como objetivo assegurar a implementação do SNMPv3, assim como é solicitado no software de gerenciamento item "9.7.22.". O SNMPv3 fornece todas as funções do SNMPv1 e SNMPv2, e apresenta um mecanismo de segurança que autentica e criptografa pacotes SNMP. Em termos de segurança, o SNMPv3 enfatiza a segurança dos dados e o controle de acesso. O SNMPv3 garante a segurança dos pacotes SNMP das seguintes maneiras:

1. Verificação da integridade dos dados Os dados não podem ser modificados de forma não autorizada. A alteração da sequência de dados é limitada à extensão permitida.

2. Autenticação de origem de dados O SNMPv3 autentica o nó gerenciado do qual a origem é recebida e não o aplicativo que gera o pacote.

3. Confidencialidade dos dados: Quando o NMS ou o agente recebe um pacote, verificam a hora em que o pacote é gerado. Se a diferença entre a hora de criação e a hora do sistema exceder o limite, o pacote será descartado. Desta forma, os pacotes que são modificados por mal-intencionados não são aceitos.

A segunda parte da sugestão é a adição de uma alternativa de protocolo de gerenciamento. A sugestão apenas acrescenta uma alternativa, não altera para os fabricantes que implementam a gerência por meio de SNMP. O NETCONF, assim como o SNMP, é um protocolo aberto e inclusive mais interoperável que o SNMP.

O Network Configuration Protocol (NETCONF) é um protocolo de gerenciamento de rede que permite que um sistema de gerenciamento de rede (NMS) entregue, modifique e exclua configurações de dispositivos de rede.

As interfaces de programação de aplicativos (APIs) padrão estão disponíveis em dispositivos de rede para que o NMS gerencie os dispositivos usando o NETCONF. Para superar as desvantagens da CLI e do SNMP, o

NETCONF baseado em XML é introduzido, que tem as seguintes vantagens:

1. NETCONF usa uma estrutura de protocolo hierárquico, tornando-o mais adequado para requisitos de big data, automatizados e sob demanda de redes baseadas em nuvem.

2. NETCONF usa codificação XML para definir mensagens e usa o mecanismo RPC para modificar dados de configuração. Isso facilita o gerenciamento de dados de configuração e a interoperabilidade entre dispositivos de diferentes fornecedores.

3. O NETCONF realiza operações em dispositivos baseados no modelo YANG, reduzindo falhas de rede causadas por erros de configuração manual.

4. NETCONF fornece mecanismos de segurança, como autenticação e autorização para garantir a segurança da transmissão de mensagens.

5. O NETCONF fornece um mecanismo de transação para oferecer suporte à classificação, armazenamento e migração de dados, envio baseado em fases, isolamento de configuração, bem como entrega, verificação e reversão de configuração geral, minimizando o impacto nos serviços de rede.

Resposta: A sugestão será acatada parcialmente:

“Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c ou SNMPv3, incluindo a geração de traps e/ ou NETCONF”

Texto Original: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 e SAE-AES;

Sugestão de Alteração: Implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal.

Justificativa: Solicitamos a alteração para termos utilizados pela Wi-Fi Alliance https://www.wi-fi.org/discover-wi-fi/security para definir os padrões de segurança WPA3. O texto sugerido possibilita a fácil compreensão e identificação ao atendimento de diversos fabricantes e engloba os modos de criptografia de 128, 192 e 256 bits.

Resposta: A sugestão será atendida parcialmente:

“Poderá ser implementado WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES ou, ainda, implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal.”

Texto Original: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem.

Sugestão de Alteração: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem em infra-estrutura privada e de uso exclusivo da Secretaria de Estado de Educação de Minas Gerais.

Justificativa: Sugestão para clarificar o modo de implementação da controladora/gerência. O texto “nuvem” pode ser interpretado como nuvem pública. Apesar de já estar descrito no software de gerenciamento

que a solução deve estar instalada em infra-estrutura da contratada para ser posteriormente migrada para a infra-estrutura da contratante, a descrição pode ser mais clara nos APs para não restar dúvidas que não serão aceitas soluções em nuvem pública.

Resposta: A sugestão não será acatada.

Texto Original: Deve incluir solução de controladora em nuvem responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários.

Sugestão de Alteração: Deve incluir solução de controladora em nuvem em infra-estrutura privada e de uso exclusivo da Secretaria de Estado de Educação de Minas Gerais responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários.

Justificativa: Sugestão para clarificar o modo de implementação da controladora/gerência. O texto "nuvem" pode ser interpretado como nuvem pública. Apesar de já estar descrito no software de gerenciamento que a solução deve estar instalada em infra-estrutura da contratada para ser posteriormente migrada para a infra-estrutura da contratante, a descrição pode ser mais clara nos APs para não restar dúvidas que não serão aceitas soluções em nuvem pública.

Resposta: A sugestão não será acatada.

Texto Original: A solução de Controladora Wireless em Nuvem deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração.

Sugestão de Alteração: A solução de Controladora Wireless em Nuvem em infra-estrutura privada e de uso exclusivo da Secretaria de Estado de Educação de Minas Gerais deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de

Referência em um mesmo console de administração.

Justificativa: Sugestão para clarificar o modo de implementação da controladora/gerência. O texto "nuvem" pode ser interpretado como nuvem pública. Apesar de já estar descrito no software de gerenciamento que a solução deve estar instalada em infra-estrutura da contratada para ser posteriormente migrada para a infra-estrutura da contratante, a descrição pode ser mais clara nos APs para não restar dúvidas que não serão aceitas soluções em nuvem pública.

Resposta: A sugestão não será acatada.

Texto Original: Fonte de energia: 100-240 V CA, 50 / 60Hz; FCC, CE, RoHS.

Sugestão de Alteração: Fonte de energia: 100-240 V CA, 50 / 60Hz; FCC, CE, RoHS. Ou injetor PoE adequado para o funcionamento do ponto de acesso externo

Justificativa: Solicitamos a alteração, sem prejuízos ao funcionamento da solução. O injetor PoE funcionará exatamente como uma fonte de alimentação para o ponto de acesso externo. Devido ao AP de ambientes externos da Huawei possuir o maior nível de proteção contra intempéries do mercado, o IP68, o AP não possui abertura desprotegida para fonte de energia. A porta de rede em que o cabo de alimentação PoE (por meio do switch PoE ou injetor PoE) é conectado é totalmente protegida contra água e poeira.

Resposta: A sugestão não será acatada.

---

3. SWITCHES

Remover o item: Auto Uplink em Cada Porta;

Justificativa: Solicitamos que o item seja removido. Em razão do termo "Auto Uplink" ser específico de um fabricante (TP-LINK), há dúvidas sobre a funcionalidade requerida. Não foram encontradas explicações profundas do fabricante sobre o que essa funcionalidade trata. Não é recomendado ter especificações que dependem de interpretação. No nosso entendimento, o termo é relacionada à funcionalidade de auto-negociação, em que as portas do switch negociam a velocidade automaticamente, já solicitada no item "24 portas RJ45 10/100/1000Mbps (Auto Negociação / Auto MDI / MDIX) e 4 portas SFP 1G com fornecimento de transceiver BASESR; BASE-SR (300-400m);"

Resposta: A sugestão será acatada. O item será removido

Texto Original: Controle de Fluxo 802.3x, Back;

Sugestão de Alteração: Controle de Fluxo 802.3x.

Resposta: A sugestão será acatada. O item será removido

Texto Original: Comutação: 52 Gbps;

Sugestão de Alteração: Comutação: 56 Gbps

Justificativa: É solicitado switch de 24 portas 1G BASE-T UTP mais 4 portas 1G SFP. Para o switch ser non-blocking, ou seja, ser capaz de comutar toda comunicação de todas as portas simultaneamente em suas capacidades máximas, deve realizar comutação de 24 + 4 = 28 Gbps. Considerando a comunicação bidirecional (full-duplex), deve ter capacidade de 28 x 2 = 56 Gbps.

Resposta: Resposta: A sugestão será acatada parcialmente:

Comutação: mínimo de 52 Gbps;

Texto Original: Taxa de encaminhamento de pacotes: 36Mpps;

Sugestão de Alteração: Taxa de encaminhamento de pacotes: 42Mbps;

Justificativa: É solicitado switch de 24 portas 1G BASE-T UTP mais 4 portas 1G SFP. Para o switch ser wire-speed, ou seja, ser capaz de encaminhar todo o tráfego de todas as portas simultaneamente em suas capacidades máximas, deve possuir taxa de encaminhamento de pacotes de (28 Gbps / 8) / 84 bytes = 41.6 Mpps. A lógica do cálculo é dada por: primeiramente dividir a banda unidirecional das portas presentes por 8 para se ter o número em gigabytes por segundo, seguida da divisão pela quantidade de bytes do menor pacote possível (64 bytes de dataframe + 8 bytes de preâmbulo + 12 bytes de interframe gap = 84 bytes), obtendo o resultado em milhões de pacotes por segundo.

Resposta: A especificação será readequada:

"Taxa de encaminhamento de pacotes: mínimo de 36 Mpps

Texto Original: Jumbo Frame: 10KB;

Sugestão de Alteração: Jumbo Frame: 9KB;

Justificativa: Solicitamos alteração de Jumbo Frames para 9KB. A pequena alteração não afetará no funcionamento da solução e limita a participação de fabricantes com equipamentos adequados ao porte das escolas.

Resposta: A sugestão será acatada, será alterada para 9KB.

Texto Original: 24 portas RJ45 10/100/1000Mbps (Auto Negociação /Auto MDI / MDIX) e 4 portas SFP 1G com fornecimento de transceiver BASESR; BASE-SR (300-400m);

Sugestão de Alteração: 24 portas RJ45 10/100/1000Mbps (Auto Negociação /Auto MDI / MDIX) e 4 portas SFP 1G populadas com transceivers BASESR; BASE-SR (300-400m); Ou

24 portas RJ45 10/100/1000Mbps (Auto Negociação /Auto MDI / MDIX) e 4 portas SFP 1G com fornecimento de 1 transceiver BASESR; BASE-SR (300-400m) por switch;

Justificativa: Sugerimos a descrição mais clara de quantos transceivers devem ser fornecidos por switch.

Resposta: A especificação será readequada:

24 portas RJ45 10/100/1000Mbps (Auto Negociação/ Auto MDI/ MDIX) e 4 portas SFP 1G com fornecimento de transceivers BASESR; BASE-SR (300-400m) 1 para switch e 1 para ponto de acesso externo.

Texto Original: Implementar o padrão PoE em todas as 24 portas RJ-45, com potência energética necessária nas portas PoE a fim de atender na plenitude o funcionamento dos AP`s;

Sugestão de Alteração: Implementar o padrão PoE em todas as 24 portas RJ-45, com potência energética necessária nas portas PoE a fim de atender simultaneamente todas as 24 portas do switch em 802.3af. A potência PoE entregue pelo switch deve atender no mínimo 10 APs internos e 1 AP externo.

Justificativa: Sugerimos que seja solicitado no mínimo o funcionamento simultâneo de todas as 24 portas em 15.4 W (802.3af), para efeito de preservação de investimento, o equipamento pode servir para alimentar câmeras ou outros dispositivos PoE, sendo uma característica básica dos switches de entrada dos mais diversos fabricantes.

Ainda, deve ser assegurado que o switch atenda à potência necessária para os APs, caso ultrapasse o total previsto sugerido (15.4W x 24 = 370W). A potência de PoE para atender na plenitude o funcionamento dos AP's é dependente da quantidade de APs que serão alimentados, por exemplo, supondo que os APs internos e externos ofertados por determinado fabricante possuam especificação de consumo máximo de 15W (padrão 802.3af) e 30W (padrão 802.3at), respectivamente. Para alimentar 5 APs internos e 1 AP externo são necessários 105W de potência de PoE no switch. Caso os APs ofertados utilizem maior potência de alimentação, a lógica do cálculo é a mesma e pode ultrapassar os 370W previstos. Para o participante do certame fazer o cálculo corretamente, é necessário indicar as quantidades de APs, sendo assim, sugerimos a

alteração para clarificar a quantidade máxima de APs prevista em cada switch.

Resposta: A sugestão não será acatada

Sugestão de Adição: Implementar 2000 VLANs ativas/ Implementar 2000 ACLs ativas.

Justificativa: A implementação de VLANs e ACLs no switch são características básicas para a implementação de redes seguras e controladas nas escolas. A sugestão é baseada nas melhores práticas elaboradas por décadas de experiência da Huawei. O objetivo principal do projeto é prover cobertura wireless de qualidade para todas as escolas, um recurso poderoso para fugir do controle da SEE ou ser implementado sem a devida preocupação com segurança.

Nas escolas temos o acesso de estudantes, professores, profissionais administrativos, profissionais comuns (ex. limpeza e manutenção), visitantes (ex: pais e eventos), etc. Normalmente essas redes são separadas em

diferentes SSIDs, mas, para segmentar de fato a rede desses diversos usuários, é necessário associar cada SSID a uma VLAN diferente. Ainda, é recomendado segmentar a rede de endpoints como câmeras, como premissa básica de segurança, já que as credenciais desses endpoints podem ser facilmente quebradas, e na ocasião da implementação de uma rede única, a invasão à rede pode facilmente se estender a todos os equipamentos conectados, incluindo computadores administrativos e de professores. A implementação de ACL assegura a utilização dos recursos da rede aos devidos usuários privilegiados e autenticados, também contribuindo para a segurança da rede.

Os valores solicitados são pequenos, os equipamentos Huawei implementam muito mais recursos de VLAN e de ACL. A sugestão visa assegurar a qualidade da implementação do projeto, independente do vencedor do certame.

Resposta: A sugestão não será acatada.

9.7 - SOLUÇÃO DE GERENCIAMENTO

Texto Original:

9.7.1. Os equipamentos devem incluir Solução de Gerência da Rede Sem Fio deve ser fornecida em Appliance Virtual;

9.7.8. A solução deverá ser disponibilizada através da imagem de sistema operacional, já com os softwares necessários para a instalação em

VMWARE.

Sugestão de Alteração: Substituir os itens 9.7.1 e 9.7.8 por:

9.7.8. Deverão ser providos quantos softwares e ou appliance forem necessários para realizar as funções de gerenciamento e controle de todos os pontos de acesso e switches contratados, incluindo sistema operacional e todas as licenças necessárias.

Justificativa: A solução ofertada deve incluir os appliances, softwares, sistema operacional e sistemas de virtualização necessários ao funcionamento da solução, não havendo motivos para limitar o tipo de Hypervisor utilizado. Dessa forma, solicitamos a alteração para que todos os recursos para o funcionamento pleno da solução sejam entregues, de acordo com as especificações dos diferentes fabricantes.

Resposta: A especificação do subitem 9.7.8. será readequada:

"9.7.8. A solução deverá ser disponibilizada através da imagem de sistema operacional, já com os softwares e licenças necessárias para a instalação em VMWARE."

Texto Original: 9.7.4. A solução deve suportar e estar licenciado para gerenciar todos os APs E switches constantes neste termo de referência;

Sugestão de Alteração: 9.7.4. A solução deve suportar gerenciar todos os APs E switches constantes neste termo de referência;

Justificativa: O item original é ligeiramente contraditório com o item seguinte "9.7.5. Deve ser licenciado em quantidade unitária, sendo uma licença por dispositivo a ser gerenciado.". Financeiramente é mais vantajoso para o cliente o licenciamento unitário, uma vez que trata-se de uma ATA de registro de preço, em que as aquisições são feitas em partes. Não é vantajoso pagar pelo software de gerenciamento licenciado para a quantidade total de equipamentos sem ter a certeza de aquisição dessa quantidade de equipamentos (APs e switches). Assim, sugerimos a alteração no item para reforçar o licenciamento unitário, já solicitado no item 9.7.5.

Resposta: A sugestão será desconsiderada, pois não existem discrepâncias entre o texto original e a sugestão.

Texto Original: 9.7.7. A solução deve estar instalada em infraestrutura da CONTRATADA podendo ser migrado para infraestrutura da CONTRATANTE no término do contrato ou quando for solicitado.

Sugestão de Alteração: 9.7.7. A solução deve estar instalada em infraestrutura sob responsabilidade da CONTRATADA podendo ser migrado para infraestrutura da CONTRATANTE no término do contrato ou quando for solicitado.

Justificativa: Sugerimos a alteração para a possibilidade da contratação de ambientes de ISPs para implementação da infra-estrutura, com o fornecimento de ambiente especializado para os equipamentos.

Resposta: A sugestão não será acatada

Texto Original: 9.7.2. Deve ser obrigatoriamente do mesmo fabricante dos pontos de acesso;

Sugestão de Alteração: 9.7.2. Deve ser obrigatoriamente do mesmo fabricante dos pontos de acesso e dos switches

Justificativa: Sugerimos a utilização de uma solução unificada e centralizada dos ativos (APs e switches) do projeto.

Resposta: A sugestão não será acatada.

Texto Original:

9.7.11. Possuir capacidade de projeto automatizado de redes sem fio nos padrões 802.11a, 802.11b e 802.11g, 802.11n, 802.11ac e 802.11ax, segundo a geografia do prédio;

9.7.12. Considerar a área de cobertura e a banda por usuário desejada;

9.7.14. Permitir a visualização de eventuais áreas sem cobertura de RF (áreas de sombra);

9.7.17.2. Visualização do mapa de calor de RF (Heatmap);

9.7.29. Possibilitar a identificação de paredes e divisórias com respectivos níveis de atenuação por tipo (alvenaria, vidro, drywall e divisória);

Sugestão de Alteração: Sem alteração de texto, alteração de posição

Justificativa: A ferramenta da Huawei de planejamento da rede sem fio com visualização da planta baixa dos andares é um software independente e integrável à solução de gerenciamento, encaixando-se na condição descrita pelo subitem "9.7.17.5. Caso esta funcionalidade não esteja disponível no sistema de gerência, deve ser fornecido software, do mesmo fabricante, para atender este item.". Sendo assim, solicitamos que os itens listados acima sejam subitens do item 9.7.17''. Deve possuir informação visual e gráfica, planta baixa dos andares, para:", sem prejuízos ao funcionamento da solução.

Resposta: A sugestão será desconsiderada, pois não foi solicitada alterações

---

Texto Original: 9.7.20. Possuir capacidade de geração de relatórios dos seguintes tipos:

Sugestão de Alteração: 9.7.20. Possuir capacidade de geração de relatórios ou visualização na interface gráfica das seguintes informações:

Justificativa: Solicitamos a alteração para participação.

Resposta: A sugestão será acatada

Texto Original: 9.7.20.6. Suportar SSH, HTTP/HTTPS, SSL, Telnet;

Sugestão de Alteração: Fazer do item um novo tópico.

Justificativa: No texto original o item mencionado é subitem de 9.7.20. Possuir capacidade de geração de relatórios dos seguintes tipos:". Para coerência do texto, sugerimos que seja removido dos subitens do item 9.7.20.

Resposta: A sugestão será acatada.

Criar novo tópico: Suportar SSH, HTTP/HTTPS, SSL, Telnet;

Texto Original: 9.7.22 Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c ou SNMPv3, incluindo a geração de traps;

Sugestão de Alteração: 9.7.22. Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps, ou NETCONF.

Justificativa: A primeira parte da sugestão tem como objetivo assegurar a implementação do SNMPv3, assim como é solicitado no software de gerenciamento item "9.7.22.". O SNMPv3 fornece todas as funções do SNMPv1 e SNMPv2, e apresenta um mecanismo de segurança que autentica e criptografa pacotes SNMP. Em termos de segurança, o SNMPv3 enfatiza a segurança dos dados e o controle de acesso. O SNMPv3 garante a segurança dos pacotes SNMP das seguintes maneiras:

1. Verificação da integridade dos dados, os dados não podem ser modificados de forma não autorizada. A alteração da sequência de dados é limitada à extensão permitida.

2. Autenticação de origem de dados O SNMPv3 autentica o nó gerenciado do qual a origem é recebida e não o aplicativo que gera o pacote.

3. Confidencialidade dos dados: Quando o NMS ou o agente recebem um pacote, verificam a hora em que o pacote é gerado. Se a diferença entre a hora de criação e a hora do sistema exceder o limite, o pacote será descartado. Desta forma, os pacotes que são modificados por mal-intencionados não são aceitos.

A segunda parte da sugestão é a adição de uma alternativa de protocolo de gerenciamento. A sugestão apenas acrescenta uma alternativa, não altera para os fabricantes que implementam a gerência por meio de SNMP. O NETCONF, assim como o SNMP, é um protocolo aberto e inclusive mais interoperável que o SNMP.

O Network Configuration Protocol (NETCONF) é um protocolo de gerenciamento de rede que permite que um sistema de gerenciamento de rede (NMS) entregue, modifique e exclua configurações de dispositivos de rede.

As interfaces de programação de aplicativos (APIs) padrão estão disponíveis em dispositivos de rede para que o NMS gerencie os dispositivos usando o NETCONF. Para superar as desvantagens da CLI e do SNMP, o

NETCONF baseado em XML é introduzido, que tem as seguintes vantagens:

1. NETCONF usa uma estrutura de protocolo hierárquico, tornando-o mais adequado para requisitos de big data, automatizados e sob demanda de redes baseadas em nuvem.

2. NETCONF usa codificação XML para definir mensagens e usa o mecanismo RPC para modificar dados de configuração. Isso facilita o gerenciamento de dados de configuração e a interoperabilidade entre dispositivos de diferentes fornecedores.

3. O NETCONF realiza operações em dispositivos baseados no modelo YANG, reduzindo falhas de rede causadas por erros de configuração manual.

4. NETCONF fornece mecanismos de segurança, como autenticação e autorização para garantir a segurança da transmissão de mensagens.

5. O NETCONF fornece um mecanismo de transação para oferecer suporte à classificação, armazenamento e migração de dados, envio baseado em fases, isolamento de configuração, bem como entrega, verificação e reversão de configuração geral, minimizando o impacto nos serviços de rede.

Resposta: A sugestão será acatada parcialmente:

"Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c ou SNMPv3, incluindo a geração de traps e/ ou NETCONF"

Texto Original:

9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance, sendo compatível com os seguintes Hypervisors:

9.8.1.1. VmWare ESXi 5.5 ou superior;

9.8.1.2. Microsoft Hyper-V Server 2012 R2/2016 e Windows Server 2012 R2 com Hyper-V;

9.8.1.3. Amazon EC2;

9.8.1.4. CentOS KVM;

Sugestão de Alteração: 9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance. Deverão ser providos quantos softwares e ou appliance forem necessários para realizar as funções de gerenciamento e controle de todos os pontos de acesso e switches contratados, incluindo sistema operacional e todas as licenças

necessárias.

Justificativa: A solução ofertada deve incluir os appliances, softwares, sistema operacional e sistemas de virtualização necessários ao funcionamento da solução, não havendo motivos para limitar o tipo de Hypersor utilizado. Dessa forma, solicitamos a alteração para que todos os recursos para o funcionamento pleno da solução sejam entregues, de acordo com as especificações dos diferentes fabricantes.

Resposta: A especificação será readequada

"9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance. Deverão ser providos quantos softwares e ou appliance forem necessários para realizar as funções de gerenciamento e controle de todos os pontos de acesso e switches contratados, incluindo sistema operacional e todas as licenças necessárias. "

Texto Original: 9.8.3. A solução deve ser disponibilizada em infraestrutura da CONTRATADA, devendo ser

transferida para infraestrutura da CONTRATANTE ao fim do contrato ou quando for solicitado.

Sugestão de Alteração: 9.7.7. A solução deve estar instalada em infraestrutura sob responsabilidade da CONTRATADA podendo ser migrado para infraestrutura da CONTRATANTE no término do contrato ou quando for solicitado.

Justificativa: Sugerimos a alteração para a possibilidade da contratação de ambientes de ISPs para implementação da infraestrutura, com o fornecimento de ambiente especializado para os equipamentos.

Resposta: A sugestão será desconsiderada, pois ambos os textos "Original e Sugestão de Alteração", constam como textos originais no Termo de Referência.

Texto Original: 9.8.5. Possuir plataforma unificada que combina AAA, NAC, BYOD e acesso de convidado incorporando identidade, integridade, informações físicas/ de dispositivo e elementos condicionais em um conjunto de políticas.

Sugestão de Alteração: 9.8.5 Possuir plataforma unificada que combina AAA e controle de acesso de usuários convidados.

Justificativa: Solicitamos a substituição pelo texto simplificado para fácil constatação ao atendimento às funcionalidades requeridas através da documentação dos diversos fabricantes. O texto original contém termos que dependem de interpretação. O texto sugerido é claro sobre a solução que está sendo solicitada, com termos utilizados pelos mais diversos fabricantes.

Resposta: A especificação será readequada:
"9.8.5 Possuir plataforma unificada que combina AAA e controle de acesso de usuários convidados."

Texto Original:

9.8.6. Suporte a seguintes fontes para autenticação:

9.8.6.1. Microsoft Active Directory

9.8.6.2. Kerberos

9.8.6.3. LDAP-compliant directory

9.8.6.4. ODBC-compliant SQL server

9.8.6.5. Token servers

9.8.6.6. Base SQL interna

9.8.6.7. Radius

9.8.6.8. Microsoft Azure Active Directory

9.8.6.9. Google G Suite

9.8.6.10. HTTP

9.8.6.11. Lista estática de endereços MAC autenticação:

Sugestão de Alteração:

9.8.6. Suporte a seguintes fontes para autenticação:

9.8.6.1. Microsoft Active Directory

9.8.6.2. LDAP

9.8.6.3. Base SQL interna

9.8.6.4. Radius

9.8.6.5. Google G Suite

9.8.6.6. HTTP

9.8.6.7. Lista estática de endereços MAC autenticação:

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A sugestão será acatada.

Para o item 9.8.6 e seus subitens serão consideradas as especificações a seguir:

9.8.6. Suporte a seguintes fontes para autenticação:

9.8.6.1. Microsoft Active Directory

9.8.6.2. LDAP

9.8.6.3. Base SQL interna

9.8.6.4. Radius

9.8.6.5. Google G Suite

9.8.6.6. HTTP

9.8.6.7. Lista estática de endereços MAC autenticação

Texto Original: 9.8.8. Registro e autenticação de usuário baseado na Web (como autor-registro, sponsor based e social-login).

9.8.8.1. Multifator de autenticação OnConnect

Sugestão de Alteração: 9.8.8. Registro e autenticação de usuário baseado na Web, por meio de auto-registro ou login através de rede social.

9.8.8.1. Multifator de autenticação

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: Para o item 9.8.8. A especificação será readequada:

"9.8.8. Registro e autenticação de usuário baseado na Web, por meio de auto-registro ou login através de rede social."

Resposta: Para o item 9.8.8.1. A especificação será readequada:
"9.8.8.1. Multifator de autenticação"

Remover item: 9.8.9. Recursos do 360 Security Exchange, incluindo servidores de contexto de endpoint locais e ações de servidor de contexto para o host local e XML.

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A especificação será readequada:

"A solução de autenticação deve permitir integração com ferramentas de segurança de terceiros, tipo antivírus, firewall"

Remover item: 9.8.10. Demais recursos devem ser suportados através de upgrades futuros da solução.

Justificativa: Sugerimos a remoção do item. O item não é claro sobre quais recursos devem ser suportados através de upgrades futuros, abrindo espaço para interpretações e entregas de software sem todas as capacidades solicitadas para o projeto.

Resposta: A sugestão não será acatada.

Texto Original: 9.8.12. Permitir a visualização de todas informações relativas a cada transação/autenticação em uma única tela, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise.

Sugestão de Alteração: 9.8.12. Permitir a visualização de todas informações relativas a cada transação/autenticação, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise.

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A sugestão será acatada.

"9.8.12. Permitir a visualização de todas informações relativas a cada transação/autenticação, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise."

Texto Original: 9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authentication;

Sugestão de Alteração: 9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ ou HWTACACS e Web Authentication;

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A especificação será readequada.

“9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ ou similar e Web Authentication;”

Texto Original: 9.8.17. Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex.

Computador, Smartdevice, impressora, etc), por sistema operacional (ex. Windows, Linux, MacOS, etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server, etc);

Sugestão de Alteração: 9.8.17. Deve categorizar os dispositivos, por tipo de dispositivo (ex. Computador, Smart device, impressora, etc.) e por sistema operacional;

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A especificação será readequada:

“9.8.17. Deve categorizar os dispositivos, por tipo de dispositivo (ex. Computador, Smart device, impressora, etc.) e por sistema operacional”

Texto Original: 9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting;

Sugestão de Alteração: 9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, SNMP e base de assinaturas;

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A especificação será readequada:

“9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, SNMP e base de assinaturas;”

Texto Original: 9.8.21. Deve implementar os serviços de autenticação, profiling e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos.

Sugestão de Alteração: 9.8.21. Deve implementar os serviços de autenticação, profiling e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos e até 700.000 (setecentos mil) usuários/dispositivos online, na implementação completa de todas as escolas previstas;

Justificativa: A solução da Huawei de controle de acesso suporta até 2.000.000 (dois milhões) de usuários, e, em sua configuração máxima, até 700.000 (setecentos mil) usuários online. É importante para o projeto ressaltar a diferença entre usuários totais e usuários online na especificação. Sugerimos o esclarecimento.

Resposta: A sugestão não será acatada.

Texto Original:

9.8.25. Deve suportar no mínimo os seguintes métodos de autenticação:

9.8.25.1. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)

9.8.25.2. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAPPEAP-Public, EAP-PWD)

9.8.25.3. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)

9.8.25.4. EAP-TLS

9.8.25.5. PAP, CHAP, MSCHAPv1, MSCHAPv2 and EAP-MD5

9.8.25.6. Windows machine authentication

9.8.25.7. SMB v2/v3

9.8.25.8. WPA3 - MPSK

9.8.25.9. RADSec

9.8.25.10. Online Certificate Status Protocol (OCSP)

9.8.25.11. TACACS+

9.8.25.12. WEB Authentication

Sugestão de Alteração:

9.8.25. Deve suportar no mínimo os seguintes métodos de autenticação:

9.8.25.1. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);

9.8.25.2. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP);

9.8.25.3. WPA3

9.8.25.4. TACACS+ ou HWTACACS

9.8.25.5. WEB Authentication

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A sugestão será acatada. Para o item 9.8.25 e seus subitens a especificação será alterada conforme a seguir:

9.8.25. Deve suportar no mínimo os seguintes métodos de autenticação:

9.8.25.1. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);

9.8.25.2. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP);

9.8.25.3. WPA3

9.8.25.4. TACACS+ ou similar

9.8.25.5. WEB Authentication

Texto Original:

9.8.29. Suporte aos seguintes recursos através de IPv6:

9.8.29.1. Administração via WEB e CLI

9.8.29.2. Servidores de autenticação e autorização com endereçamento IPv6;

9.8.29.3. IPv6 Accounting Proxy;

9.8.29.4. Acesso a servidores com endereçamento IPv6 para contexto de endpoints;

9.8.29.5. Syslog, DNS, NTP;

9.8.29.6. Endereçamento IPv6 para VIP (Virtual IP) de alta disponibilidade;

9.8.29.7. Fontes de Syslog para processamento de evento

Sugestão de Alteração: Substituir o item 9.8.29. e seus subitens por:

9.8.29. Suporte a servidores de autenticação e autorização com endereçamento IPv6;

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A sugestão será acatada parcialmente:
9.8.29. Suporte a servidores de autenticação e autorização com endereçamento IPv6;

9.8.29.1. Fontes de Syslog para processamento de evento

Remover o item: 9.8.29.8. Validações e conformidades:

9.8.29.8.1. FIPS 140-2

9.8.29.8.2. Common Criteria NDcPP + Servidor de autenticação

Justificativa: Solicitamos a remoção para participação no certame.

Resposta: A sugestão será acatada.

Texto Original: 9.8.31. A solução deve permitir a configuração centralizada de políticas em ambientes distribuídos, no qual as políticas serão configuradas em um único elemento para serem distribuídas aos demais que pertençam à mesma "zona"

Sugestão de Alteração: 9.8.31. A solução deve permitir a configuração centralizada de políticas em ambientes distribuídos, no qual as políticas serão configuradas em um único elemento para serem distribuídas aos demais que pertençam a um mesmo grupo

Justificativa: Solicitamos a remoção para participação no certame.

Resposta: A sugestão não será acatada.

Texto Original: 9.8.33. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML e PDF.

Sugestão de Alteração: 9.8.33. A solução deve possuir ferramenta para

geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML ou PDF ou CSV ou EXCEL.

Justificativa: Solicitamos a remoção para participação no certame.

Resposta: A especificação será readequada:

9.8.33. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML ou CSV ou EXCEL e PDF.

ALTASNET

Texto Original: 1.2.8. Os ativos de rede (ponto de acesso, switches, nobreak) devem vir com etiqueta de patrimônio conforme modelo e range a ser fornecido pela SEE.

Comentário: Qual tipo de etiqueta? Poderá ser uma etiqueta confeccionada por uma rotuladora eletrônica, a mesma utilizada em identificação de cabeamento?

Resposta: O texto será readequado.

"1.2.8. Os ativos de rede (ponto de acesso, switches, nobreak) devem vir com etiqueta de patrimônio conforme modelo e range a ser fornecido pela SEE. Deve ser confeccionada em material resistente à abrasão, calor, poeira, umidade ou quaisquer outros fatores que possam causar deterioração, devendo constar o número e código de barras."

Texto Original: 5.1. Não será permitida a participação de empresas reunidas em consórcio, devido à baixa complexidade do serviço a ser contratado, considerando que as empresas que atuam no mercado têm condições de prestar os serviços de forma independente.

Comentário: Permitir a participação de consórcios, o valor de contratação é considerável e participação de consórcios poderia viabilizar a participação de mais proponentes. Temos o exemplo da CAMG que todo fornecimento do parque tecnológico foi mediante consórcio de empresas.

Resposta: Conforme disposto no item 5. DA PARTICIPAÇÃO DE CONSÓRCIOS não será permitida a participação de empresas reunidas em consórcio (...)

Texto Original: 7.3. Caso a compatibilidade com as especificações demandadas, sobretudo quanto a padrões de qualidade e desempenho, não possa ser aferida pelos meios previstos no subitem acima, o Pregoeiro exigirá que o licitante classificado em primeiro lugar apresente amostra, sob pena de não aceitação da proposta, no local a ser indicado e dentro de 5 (cinco) dias úteis contados da solicitação.

Comentário: "Caso ocorra qualquer dúvida não esclarecida quanto ao atendimento das especificações técnicas, a SEDUC poderá requisitar amostra de todos os itens tecnológicos ofertados, para realização de laboratório técnico, simulando o ambiente de uma escola. Os equipamentos devem ser entregues dentro do prazo de 10 dias úteis contados a partir da solicitação"

Resposta: A sugestão não será acatada.

Texto Original: 9.1.1. Os equipamentos adquiridos deverão ser entregues em até 90 (noventa) dias corridos contados do dia seguinte ao recebimento da Nota de Empenho, Autorização de Fornecimento ou documento equivalente.

Comentário: "Os equipamentos adquiridos deverão ser entregues de acordo com o cronograma."

Resposta: O item será readequado.

Texto Original: 9.6.1.2. Suporte Local – nível 2: serviço de atendimento local a chamados técnicos críticos, que deverão ser atendidos localmente, por profissional capacitado. Este serviço terá acionamento 13x5 (13 horas por dia, 5 dias por semana), das 7h – 20h

Comentário: O atendimento local em cada escola fará com que o custo do

projeto possa se tornar inviável, logo sugerimos que o atendimento local seja no ponto central da SEDUC.

Resposta: A sugestão não será acatada.

Texto Original: 9.6.12 - Tabela de Classificação de Chamadas

Severidade	Descrição	Tempo de Início de atendimento	Tempo de Solução
1. Urgente	Indisponibilidade dos ativos e identificação de falha na solução com interrupção do serviço.	Em até 04 (quatro) horas úteis	Em até 08 (oito) horas úteis

Comentário: O SLA de atendimento é bem agressivo no que tange a resolução de indisponibilidade. Por exemplo, se um nobreak queima, dependendo da localidade é impossível substituir a peça com 8 horas. O ideal é flexibilizar o SLA por região, ou por raio de distância em relação à capital. Outro ponto que o edital não deixa claro é sobre responsabilidade de vandalismo, queima por descargas de energia ou furto de algum equipamento.

Resposta: O texto será readequado.

Severidade	Descrição	Tempo de Início de atendimento	Tempo de Solução
1. Urgente	Indisponibilidade dos ativos e identificação de falha na solução com interrupção do serviço.	Em até 04 (quatro) horas úteis	Em até 08 (oito) horas úteis. 02 (dois) dias úteis: No caso de ser identificada a necessidade de troca ou substituição dos ativos

---

Texto Original: 9.7.10. Prover organização hierárquica de equipamentos, permitindo que um equipamento receba as configurações lógicas e as replique a outros equipamentos;

Comentário: "Prover organização de equipamentos através de grupos, permitindo que todos os equipamentos de um grupo recebam as mesmas configurações lógicas”

Resposta: A sugestão não será acatada.

Texto Original: 9.8.8.1. Multifator de autenticação OnConnect

Sugestão de Alteração: Suportar no processo de autenticação o uso de MFA

Resposta: A especificação será readequada:
“9.8.8.1. Multifator de autenticação”

Texto Original: 9.8.14. Para soluções compostas por mais de um servidor/appliance, deve apresentar o Status de cada elemento dos sistemas, com informações como endereço IP e data da última replicação dos dados.

Comentário: Apenas movendo esse item que estava perdido no meio da especificação do dashboard

Resposta: A sugestão será acatada, o item 9.8.14. será removido

---

Texto Original: 9.8.16. Deve implementar funcionalidade de classificação automática de dispositivos (“Device profiling”), de forma a descobrir,

classificar e agrupar os dispositivos conectados na rede;

Comentário: "Deve suportar expansão de licenciamento para implementar funcionalidade de classificação automática de dispositivos ("Device profiling"), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;

Resposta: A especificação será readequada:
"9.8.16. Deve suportar expansão de licenciamento para implementar funcionalidade de classificação automática de dispositivos, de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;"

Texto Original: 9.8.17. Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.), por sistema operacional (ex. Windows, Linux, MacOS, etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server, etc);

Comentário: "Deve suportar expansão de licenciamento para categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.), por sistema operacional (ex. Windows, Linux, MacOS, etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server, etc);

Resposta: A especificação será readequada:

9.8.17. "Deve suportar expansão de licenciamento para categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.), por sistema operacional

---

Texto Original: 9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting;

Comentário: "Deve suportar expansão de licenciamento para suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting;

Resposta: A especificação será readequada:

"9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, SNMP e base de assinaturas;"

Texto Original: 9.8.19. Deve possuir base de regras e categorias de dispositivos pré-configurada;"

Comentário: "Deve suportar expansão de licenciamento para implementar base de regras e categorias de dispositivos pré-configurada;

Resposta: O texto será removido.

Texto Original: 9.8.20. Deve suportar mecanismo de atualização das regras e categorias pré-configuradas;

Comentário: "Deve suportar expansão de licenciamento para suportar mecanismo de atualização das regras e categorias pré-configuradas;

Resposta: A sugestão será acatada.

Texto Original: 9.8.21. Deve implementar os serviços de autenticação, profiling e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos.

Sugestão de alteração: Deve implementar os serviços de autenticação e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos, simultaneamente.

Resposta: A sugestão será acatada.

"Deve implementar os serviços de autenticação e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos, simultaneamente."

Texto Original: 9.8.23. Deve permitir que cada dispositivo receba uma

chave pré-compartilhada exclusiva durante o registro do dispositivo.

Comentário: Remover este item implica em outro módulo de licenciamento para instalar certificados digitais em devices para realização de onboarding.

Resposta: O texto será removido.

Texto Original: 9.8.26. Deve suportar a verificação de vulnerabilidade através de varredura de portas (NMAP).

Sugestão de alteração: Deve suportar profiling de devices através de varredura de portas utilizando NMAP.

Resposta: A sugestão não será acatada.

Texto Original: 14.2.1. A garantia técnica deverá ser comprovada na assinatura do contrato, contemplando o período mínimo de 36 (trinta e seis) meses ON SITE contados a partir do recebimento dos equipamentos, conferência e constatação de conformidade com as especificações pela CONTRATANTE, e por fim, atesto da Nota Fiscal relativa à entrega do lote dos equipamentos fornecidos.

Comentário: "Deve possuir garantia de fábrica do tipo Limited Life time, contemplando 5 anos de substituição de equipamentos defeituosos após o fabricante anunciar o encerramento do ciclo de vendas do produto ofertado;"

Resposta: A sugestão não será acatada.

Texto Original: 14.2.2. O atendimento será do tipo On-site mediante manutenção corretiva nas dependências da CONTRATANTE, em dias úteis (segunda-feira a sexta-feira), entre 08h00min e 17h00min, por profissionais especializados e deverá cobrir todo e qualquer defeito apresentado, incluindo o fornecimento e a substituição do equipamento, ajustes, reparos e correções necessárias, sem ônus para a CONTRATANTE.

Comentário: "O atendimento será do tipo On-site, prestado pela CONTRATADA, mediante manutenção corretiva nas dependências da CONTRATANTE, em dias úteis (segunda-feira a sexta-feira), entre 08h00min e 17h00min, por profissionais especializados e deverá cobrir todo e qualquer defeito apresentado, incluindo o fornecimento e a substituição do equipamento, ajustes, reparos e correções necessárias, sem ônus para a CONTRATANTE"

Resposta: O texto será readequado:

"14.2.2. O atendimento será do tipo On-site mediante manutenção corretiva em todas as localidades nos quais os equipamentos forem instalados, em dias úteis (segunda-feira a sexta-feira), entre 08h00min e 17h00min, por profissionais especializados e deverá cobrir todo e qualquer defeito apresentado, incluindo o fornecimento e a substituição do equipamento, ajustes, reparos e correções necessárias, sem ônus para a CONTRATANTE."

PONTO DE ACESSO INTERNO

1. LICENCIAMENTO E GERENCIAMENTO:

Solicita a inclusão do subitem:

Sugestão: "Deve possuir garantia de fábrica do tipo Limited Life time, contemplando 5 anos de substituição de equipamentos defeituosos após o fabricante anunciar o encerramento do ciclo de vendas do produto ofertado;"

Resposta: A sugestão de inclusão não será acatada.

---

2. HARDWARE

Texto Original: Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (devendo ser utilizado cabo de segurança com chave ou similar);

Sugestão de aletração: Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (devendo ser utilizado cabo de segurança com chave ou similar); Deverá ser fornecido com Kensington ou similar;

Resposta: A sugestão de inclusão não será acatada.

---

4. SEGURANÇA

Texto Original: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 e SAE-AES;

Sugestão de alteração: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES;

Resposta: A sugestão será atendida parcialmente:

"Poderá ser implementado WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES ou, ainda, implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal."

---

5. RÁDIO

Texto Original: Deve Suportar no mínimo 512 clientes por rádio (1024 por AP)

Sugestão de alteração: Deve Suportar no mínimo 256 clientes por rádio (512 por AP)

Resposta: A especificação será readequada:

"Deve Suportar no mínimo 256 clientes por rádio (512 por AP)"

---

6. INFORMAÇÕES COMPLEMENTARES

Texto Original: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem.

Sugestão de alteração: Deve possuir suporte a captive portal web (HTTPS) de autenticação do tipo splash page externo para operar em conjunto com a solução de autenticação centralizada.

Resposta: A especificação será readequada:

Deve possuir suporte a captive portal web (HTTPS) de autenticação do tipo splash page externo para operar em conjunto com a solução de autenticação centralizada.

Texto Original: Deve incluir solução de controladora em nuvem responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários.

A solução de Controladora Wireless em Nuvem deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração.

Sugestão de alteração: 9.8.1. Para pontos de acesso que não suportem operar em modo auto gerenciado, devem ser fornecidos com controladoras virtuais ou físicas, em redundância, instalado em infraestrutura da contratada permitindo: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários. Toda a comunicação entre controladoras e access points deverá ser criptografada.

Para soluções virtualizadas, deverão fazer parte do fornecimento os servidores necessários, obedecendo às especificações mínimas recomendadas pelo fabricante para a volumetria de access points, assim como sistemas operacionais e software complementares para a completa instalação do sistema, atendendo a todas as características solicitadas.

As controladoras deverão estar licenciadas, caso necessário, para quantidade total de Pontos de Acessos descritos neste Termo de Referência e serem gerenciadas pelo item de Software de Gerenciamento deste edital.

Resposta: A sugestão não será acatada.

Texto Original: Deve implementar recursos que permitam mecanismo de autenticação através de portal Web customizável (captive portal customizável) para clientes visitantes, com usuário e senha.

Deve suportar autenticação de usuários na rede por meio de contas da Google.

Sugestão de alteração:

Deve implementar recursos que permitam mecanismo de autenticação através de portal Web customizável (captive portal customizável) para clientes visitantes, com usuário e senha, através da solução de autenticação.

O captive portal externo deve suportar autenticação de usuários na rede por meio de contas da Google.

Resposta: A sugestão não será acatada.

ITEM 2 – PONTO DE ACESSO EXTERNO

1. LICENCIAMENTO E GERENCIAMENTO:

Solicita a inclusão do subitem:

"Deve possuir garantia de fábrica do tipo Limited Life time, contemplando 5 anos de substituição de equipamentos defeituosos após o fabricante anunciar o encerramento do ciclo de vendas do produto ofertado;"

Resposta: A sugestão de inclusão não será acatada.

---

2. HARDWARE

Texto Original: Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (devendo ser utilizado cabo de segurança com chave ou similar);

Capacidade de temperatura de operação de no mínimo 50°C.

Sugestão: Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (devendo ser utilizado cabo de segurança com chave ou similar). Deverá ser fornecido com Kensington ou similar. Capacidade de temperatura de operação de no mínimo 55°C.

Resposta: A sugestão de inclusão não será acatada.

---

4. SEGURANÇA

Texto Original: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 e SAE-AES;

Sugestão de inclusão: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES;

Resposta: A sugestão será atendida parcialmente:

"Poderá ser implementado WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES ou, ainda, implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal."

---

5. RÁDIO

Texto Original: Possuir antenas internas com ganho mínimo de 2,5dBi em 2,4GHz e 3 dBi em 5GHz;

Deve suportar potência máxima de transmissão de no mínimo 17.5 dBm na frequência 2.4 GHz e de no mínimo 17.5 dBm na frequência 5 GHz;

Sugestão de alteração: Possuir antenas internas com ganho mínimo de 3 dBi em 2,4GHz e 5 dBi em 5GHz;

Deve suportar potência máxima de transmissão de no mínimo 20 dBm na frequência 2.4 GHz e de no mínimo 20 dBm na frequência 5 GHz;

Resposta: A sugestão não será acatada.

---

6. INFORMAÇÕES COMPLEMENTARES

5) Texto Original: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem.

Sugestão de inclusão: Deve possuir suporte a captive portal web (HTTPS) de autenticação do tipo splash page externo para operar em conjunto com a solução de autenticação centralizada.

Resposta: A sugestão será acatada.

Texto Original: Deve incluir solução de controladora em nuvem responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários. A solução de Controladora Wireless em Nuvem deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração.

Sugestão de alteração: 9.8.1.Para pontos de acesso que não suportem operar em modo auto gerenciado, devem ser fornecidos com controladoras virtuais ou físicas, em redundância, instalado em infraestrutura da contratada permitindo: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência),funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários. Toda a comunicação entre controladoras e access points deverá ser criptografada.

Para soluções virtualizadas, deverão fazer parte do fornecimento os servidores necessários, obedecendo às especificações mínimas recomendadas pelo fabricante para a volumetria de access points, assim como sistemas operacionais e software complementares para a completa instalação do sistema, atendendo a todas as características solicitadas.

As controladoras deverão estar licenciadas, caso necessário, para quantidade total de Pontos de Acessos descritos neste Termo de Referência e serem gerenciadas pelo item de Software de Gerenciamento deste edital.

Resposta: A sugestão não será acatada.

Texto Original: Deve implementar recursos que permitam mecanismo de autenticação através de portal Web customizável (captive portal customizável) para clientes visitantes, com usuário e senha.

Deve suportar autenticação de usuários na rede por meio de contas da Google.

Sugestão de alteração: Deve implementar recursos que permitam mecanismo de autenticação através de portal Web customizável (captive portal customizável) para clientes visitantes, com usuário e senha, através da solução de autenticação.

O captive portal externo deve suportar autenticação de usuários na rede por meio de contas da Google.

Resposta: A sugestão não será acatada.

ITEM 3 – SWITCHES

Texto Original: Temperatura de operação: 0 – 40°C;

Sugestão de alteração: Temperatura de operação: 0 – 45°C

Resposta: A sugestão não será acatada.

Solicita a inclusão do subitem: Deve possuir garantia de fábrica do tipo Limited Life time, contemplando 5 anos de substituição de equipamentos defeituosos após o fabricante anunciar o encerramento do ciclo de vendas do produto ofertado;

Resposta: A sugestão de não será acatada.

---

3) Solicita a inclusão dos subitens:

2. CARACTERÍSTICAS LÓGICAS

2.1. Deve ser do gerenciado pela mesma solução de gerenciamento dos Access Points.

2.2. Deve permitir o gerenciamento local através de interface gráfica Web no padrão HTTPS e via CLI via SSHv2

2.3. Deve suportar o padrão 802.1Q com até 512 VLANs simultâneas;

2.4. Deve suportar prevenção de loops através dos protocolos de SpanningTree STP, RSTP, MSTP e RPVST+;

2.5. Deve implementar proteções no SpanningTree de root guard;

2.6. Deve suportar DHCP snooping;

2.7. Deve suportar ACL's e QoS em IPv4 e IPv6;

2.8. Deve suportar 200 ACL's em IPv4 e 100 ACL's em IPv6;

2.9. Deve suportar padrão 802.3ad LACP suportando 8 grupos de agregações com no mínimo 3 portas em cada;

2.10. Deve suportar espelhamento de porta para entrada e saída de tráfego, com no mínimo 4 grupos;

2.11. Deve suportar duas imagens de software em flash, como primária e backup;

2.12. Deve suportar armazenamento de múltiplos arquivos de configurações a flash;

2.13. Deve suportar SNMP v1, v2c e v3

Resposta: sugestão de inclusão não será acatada.

COMPWIRE

1. AP INDOOR

a. Adicionar no TR a entrega da instalação da trava de segurança para cada AP.

Resposta: A informação já consta na especificação.

---

2. AP OUTDOOR

a. Adicionar no TR a entrega da instalação da trava de segurança para cada AP.

Resposta: A informação já consta na especificação.

b. Colocar porta no mínimo 1GE com SFP para conectar fibra óptica, normalmente Aps Outdoor estão em distâncias acima de 100 mts, onde cabos UTP não conseguiram atender.

Resposta: A especificação será readequada:
"Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior e uma interface 1G SFP. Deve ser fornecido transceiver, caso o modelo não suporte conexão direta da fibra BASESR; BASE-SR (300-400m)."

---

3. SWITCH

a. Padronizar o menor switch em 24 portas

Resposta: Já está padronizada em 24 portas.

b. Especificar que o switch seja POE, eliminará os riscos de ter injetor POE. Texto está no TR em anexo (Possuir capacidade de fornecer alimentação PoE 802.3af, 802.3at ou 802.3bt).

Resposta: A especificação será readequada:

Deverá possuir o padrão PoE em todas as 24 portas RJ-45, com potência energética necessária nas portas PoE a fim de atender na plenitude o funcionamento dos AP`s;

c. Colocar porta de uplink com no mínimo 1GE com suporte a fibra óptica.

Resposta: O item será removido.

---

4. SOLUÇÃO DE GERENCIAMENTO PARA SWITCHES E APS.

a. Especificar a quantidade mínima de usuários simultâneos que deverá ser suportada pela solução.

Resposta: Vide item 9.8.21, no Termo de referência

b. Especificar que todo o licenciamento deverá ser entregue para os Aps, Switches e Solução de Gerenciamento.

Resposta: Vide item 9.7.5, no Termo de referência

c. Solução somente On-premisses, pois, soluções em nuvem, param de funcionar sem renovação de suporte.

Resposta: A sugestão não será acatada.

---

5. RACK E NO-BREAK

a. Inserir estes produtos dentro de um lote junto com os serviços para adequação física das escolas.

Resposta: A sugestão não será acatada. Será mantido lote único para o certame.

b. Informar quais os fabricantes serão aceitos tanto para o no-break quanto para o Rack, existem mais de 5 fabricantes de excelente qualidade em cada item, em compensação, tem fabricantes sem nenhum tipo de certificação ou padrão de qualidade

Resposta: Serão aceitos todos os fabricantes que atenderem às especificações técnicas contidas no Termo de Referência.

CONVERGINT

Texto Original: 9.7.23. Possuir suporte a MIB II, conforme RFC 1213;

Comentário: Entendemos que esse protocolo seria para controlador físico. Está correto nosso entendimento?

Resposta: O item será removido.

Texto Original: 9.7.33.2. Suporte telefônico para abertura de chamados em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito disponibilizado pelo fabricante.

Comentário: Entendemos que poderá utilizar o representante oficial do fabricante para abertura de chamado.

Resposta: Sim, o entendimento está correto.

Texto Original:

9.8.6. Suporte às seguintes fontes para autenticação:

9.8.6.1. Microsoft Active Directory

9.8.6.2. Kerberos

9.8.6.3. LDAP-compliant directory

9.8.6.4. ODBC-compliant SQL server

9.8.6.5. Token servers

9.8.6.6. Base SQL interna

9.8.6.7. Radius

9.8.6.8. Microsoft Azure Active Directory

9.8.6.9. Google G Suite

9.8.6.10. HTTP

9.8.6.11. Lista estática de endereços MAC

Comentário: Alguns itens solicitados não fazem sentido. Solicitamos explanação.

Resposta: A especificação será readequada para o item 9.8.6 e seus subitens e serão consideradas as especificações a seguir:

9.8.6. Suporte a seguintes fontes para autenticação:

9.8.6.1. Microsoft Active Directory

9.8.6.2. LDAP

9.8.6.3. Base SQL interna

9.8.6.4. Radius

9.8.6.5. Google G Suite

9.8.6.6. HTTP

9.8.6.7. Lista estática de endereços MAC autenticação

Texto Original: 9.8.8.1. Multifator de autenticação OnConnect

Comentário: OnConnect é referência da solução da ARUBA. Solicitamos a retirada do item.

Resposta: Para o item 9.8.8.1. A especificação será readequada:
"9.8.8.1. Multifator de autenticação"

Texto Original: 9.8.9. Recursos do 360 Security Exchange, incluindo servidores de contexto de endpoint locais e ações de servidor de contexto para o host local e XML.

Comentário: 360 Security Exchange é referência da solução da ARUBA. Solicitamos a retirada do item.

Resposta: A especificação será readequada:

"A solução de autenticação deve permitir integração com ferramentas de segurança de terceiros, tipo antivírus, firewall"

Texto Original: 9.8.25.9. RADSec

Comentário: Não suportamos essa funcionalidade.

Resposta: O item será removido.

Texto Original: 9.8.26. Deve suportar a verificação de vulnerabilidade através de varredura de portas (NMAP).

Comentário: Gostaríamos de entender como seria utilizado o NMAP.

Resposta: NMAP ("Network Mapper") é um software livre que permite fazer um scan completo em uma rede, para se obter as informações de quais hosts estão nela ativos. Além disso, ele também permite fazer port scan, a fim de descobrir quais portas estão abertas, assim como fornece a informação de quais sistemas estão rodando em um dado momento.

FIBERX

Texto Original:

9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance, sendo compatível com os seguintes Hypervisors:

9.8.1.1. VmWare ESXi 5.5 ou superior;

Resposta: A especificação será readequada.

"9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance. Deverão ser providos quantos softwares e ou appliance forem necessários para realizar as funções de gerenciamento e controle de todos os pontos de acesso e switches contratados, incluindo sistema operacional e todas licenças

necessárias. "

9.8.3. A solução deve ser disponibilizada em infraestrutura da CONTRATADA, devendo ser transferida para infraestrutura da CONTRATANTE ao fim do contrato ou quando for solicitado.

Comentário: A solução de autenticação necessita ser da mesma marca da solução de gerenciamento ou aceita-se uma solução de terceiros que será administrada pela contratada desde que aderente aos requisitos solicitados?

Resposta: Caso a CONTRATADA esteja ofertando solução de gerenciamento que não possua os recursos de autenticação do item 9.8. A mesma poderá ofertar solução integrada, de terceiros, apresentando comprovação de integração entre as soluções de gerenciamento e autenticação.

Amostra.

Comentário: Será solicitada uma comprovação dos requisitos da solução por uma amostra / prova de conceito? Se sim, pode-se disponibilizar o caderno de testes?

Resposta: Vide item 8. DA APRESENTAÇÃO DE AMOSTRA, no termo de referência.

Penalidades

Comentário: Como será a aplicação de penalidades após a efetivação das entregas, visto que o pagamento se dará após concluída com sucesso esta etapa? Existe um contrato adicional para manutenção da estrutura de atendimento após a entrega e seus acordos de níveis de serviço?

Resposta: A aplicação de penalidades estão descritas no item 18 - Sanções Administrativas. Não haverá contrato adicional, apenas o contrato referente aos serviços descritos no presente Termo de Referência.

QINTESS

ITEM 1 - PONTO DE ACESSO INTERNO

Texto Original: Deve Suportar no mínimo 512 clientes por rádio (1024 por AP)

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes à participarem do processo licitatório com produtos similares tecnicamente e com a capacidade tráfego tanto de LAN quanto de WLAN compatíveis com os demais elementos especificados na solução. Esta sugestão de alteração também vai propiciar mais competitividade e economicidade no processo de compra: Deve Suportar no mínimo 256 clientes por rádio (512 por AP)

Resposta: A especificação será readequada:

"Deve Suportar no mínimo 256 clientes por rádio (512 por AP)"

Texto Original: Possuir antenas internas com ganho mínimo de 2,5dBi em 2,4GHz e 3 dBi em 5GHz;

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes à participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Possuir antenas internas com ganho mínimo de 2 dBi em 2,4 GHz e 3 dBi em 5GHz;

Resposta: A sugestão será acatada:

Possuir antenas internas com ganho mínimo de 2dBi em 2,4GHz e 3 dBi em 5GHz;

Texto Original: Fonte de energia: 100-240 V CA, 50 / 60Hz; FCC, CE, RoHS. Cabo de alimentação;

Comentário: Entendemos que o APs do tipo indoor serão alimentados através de portas PoE dos switches, portanto não sendo necessários fornecer fonte de alimentação externa para cada AP indoor da solução. Nosso entendimento está correto?

Resposta: O entendimento está correto.

ITEM 2 - PONTO DE ACESSO EXTERNO

Texto Original: Possuir antenas internas com ganho mínimo de 2,5dBi em 2,4GHz e 3 dBi em 5GHz;

Comentário: Sugestão de alteração visando maior número de fornecedores/fabricantes a participarem do processo licitatório para propiciar competitividade e economicidade no processo de compra: Possuir antenas internas com ganho mínimo de 2 dBi em 2,4 GHz e 3 dBi em 5GHz;

Resposta: A sugestão não será acatada.

ITEM 3 - SWITCHES

Texto Original: 24 portas RJ45 10/100/1000Mbps (Auto Negociação / Auto MDI / MDIX) e 4 portas SFP 1G com fornecimento de transceiver BASESR; BASE-SR (300-400m);

Comentário: Entendemos que os transceivers solicitados serão para conexão entre o switch e o AP tipo outdoor em casos de distância superior a 100 metros, e como foi definido no T.R. apenas 1 (um) AP outdoor por escola concluímos que será necessário fornecer junto com cada switch, 2 (dois) transceiver SFP de 1G. Nosso entendimento está correto?

Resposta: O entendimento está correto.

LOGICNET TECNOLOGIA

Considerando as afirmativas no processo de consulta pública:

1) Não haverá pagamento do processo ao fornecedor sem a entrega dos produtos e serviços para as escolas.

2) O orçamento tem que ser consumido no ano de 2023, não podendo ser pago em 2024.

3) Todas as escolas da listagem estão aptas para adesão a ATA, conforme filtro feito pela secretaria.

Texto Original: O item 7 do Termo de referência em seu subitem 7.1 afirma que: " 7.1 O critério de aceitação e julgamento das propostas será o de MENOR PREÇO ofertado por LOTE de acordo com as especificações e demais condições fixadas no respectivo termo de referência."

Comentários: Considerando que somente uma empresa poderá ser adjudicada, portanto, ser diretamente responsável pela entrega e implementação da solução nas 2.127 escolas, gostaríamos de destacar alguns pontos de atenção:

a) Se considerarmos 9 meses de tempo de implementação no ano de 2023, já que 3 dos 12 meses serão para o prazo de entrega dos equipamentos, a impossibilidade de fracionar em MAIS LOTES, obriga a empresa Contratada a implementar em média 236 escolas por mês ou 11 escolas por dia, mesmo considerando que não haverá nenhum percalço de infraestrutura. Ainda que haja um ótimo planejamento de execução e mão-de obra adequada, entendemos ser um número muito alto de execução diária;

b) O valor dos serviços relacionados à entrega dessas implementações será certamente muito mais alto se comparado com um processo de contratação de um número menor de escolas;

c) A contratação de uma única empresa em um único lote certamente irá restringir muito a competitividade do certame, já que somente empresas de maior porte conseguirão participar do certamente (capital social, atestados de capacidade técnica capazes de atender ao percentual exigido, etc), ainda que isso não signifique garantia de competência técnica suficiente para melhor implementação e entrega das soluções nas escolas

d) A gestão por parte do SEE/MG ficaria muito mais fácil de gerir e acompanhar para o aceite de trabalho visto que poderiam dividir em menos pessoas para gestão dessa entrega, onde no pior caso cada gestor aprovaria 06 escolas por dia. Garantindo assim ao Estado uma qualidade na entrega do serviço e pagamento.

e) A divisão em lotes não impede que uma única empresa participe e ganhe todos os lotes, como aconteceu com a Logicnet no certame do MPMG onde levamos o lote 01 e 02, agregando ao ministério uma excelente aquisição de produtos.

f) A divisão em lote garante ao SEE/MG e as empresas que ao longo do processo, problemas que venham acontecer possam ser ajustados, contornados para cumprimento de 100% das escolas previstas, visto que o risco ficaria diluído em mais empresas, permitindo assim situações de contorno.

g) A SEE/MG não corre o risco de ter vários fabricantes participando, visto que dividido em lotes ela poderia ter no extremo da situação até 4 produtos, coisa que não iria impactar na equipe técnica do SEE/MG e também reduziria o risco de uma falha em 1 fabricante pararia todas as

escolas.

Abaixo segue estudo prático para o pleito:

Divsão Lotes	Qtde escola por lote	Qtde escola Mês por lote	Qtde escola dia por lote	jan./23	fev./23	mar./23	abr./23	mai/23	jun./23	jul./23	ago./23	set./23	out./23	nov./23	dez./23
2	1064	118	6	Pedido compra	Embarque	Embarque	118	118	118	118	118	118	118	118	118
3	709	79	4	Pedido compra	Embarque	Embarque	79	79	79	79	79	79	79	79	79
4	532	59	3	Pedido compra	Embarque	Embarque	59	59	59	59	59	59	59	59	59

Diante do exposto acima, sugerimos que seja avaliado nosso pedido para que a contratação seja realizada em lotes, pois acreditamos que trará mais competitividade ao certamente e segurança de execução ao contratado e ao mesmo tempo não impede que uma empresa ganhe todos os lotes.

Resposta: As sugestões não serão acatadas. Conforme explicitado no subitem 2.1.3, no Termo de Referência: "Observando os critérios de divisibilidade, informamos que o agrupamento dos itens respeita a legislação vigente e garantem a ampla participação das empresas existentes no mercado, sem prejuízo para o projeto ou perda de economia de Escala"

DO PROCESSO

Pergunta: Quanto ao atestado de capacidade técnica no valor de 10%. Este número representa a quantidade de escolas e não dos ativos que serão fornecidos, correto?

Resposta: O valor refere-se ao quantitativo mínimo de 10% (dez por cento) dos itens ofertados. Sendo admitido o somatório de atestados, desde que compatíveis com as características do objeto da licitação. Vide item 6. QUALIFICAÇÃO TÉCNICA, no Termo de Referência.

Pergunta: Visto que não tem um projeto definido a utilização de equipamento indoor e outdoor será feito definido pela secretaria, correto?

Resposta: O entendimento está correto.

Pergunta: Visto que não tem um quantitativo definido porque está excluindo o benefício da micro e pequena empresa?

Resposta: Vide item 2.2. LOTES EXCLUSIVOS PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

Pergunta: 2.2.5. Por se tratar de um ambiente descentralizado, no qual cada SRE terá a responsabilidade de gerenciar o sistema de conectividade das escolas sob sua jurisdição, a reserva de um percentual para ME/EPP afronta o princípio da razoabilidade e economicidade.

Resposta: Vide item 2.2. LOTES EXCLUSIVOS PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

Pergunta: A solução é toda em nuvem, esta justificativa não se aplica e é um descabimento. Entendemos que fere a regulamentação legal. Assim solicitamos que seja retirado este item, pois não é verdade a afirmativa acima.

Resposta: A sugestão não será acatada.

ITEM 1 - PONTO DE ACESSO INTERNO

1. LICENCIAMENTO E GERENCIAMENTO:

Texto Original: Deve ser certificado pela WIFI Alliance na subcategoria Enterprise/Service Provider Access Point, Switch/Controller or Router.

Dúvida: Entendemos que cada país possui um órgão regulamentador como por exemplo a ANATEL no Brasil, portanto entendemos que serão aceitos os produtos com homologação ANATEL, além disso o produto ofertado é desenvolvido conforme normativas do IEEE, que regulamenta

mundialmente os protocolos de interoperabilidade entre dispositivos wireless e cabeados garantindo assim a interoperabilidade entre equipamentos que implementam os devidos protocolos. Está correto o nosso entendimento?

Resposta: O entendimento não está correto. A certificação WIFI Alliance, na subcategoria Enterprise/Service Provider Access Point, Switch/Controller or Router pode ser requerida por qualquer fornecedor.

Texto Original: Deve possuir o certificado de Conectividade Wi-Fi CERTIFIED 6 ™ da WIFI Alliance;

Dúvida: Entendemos que cada país possui um órgão regulamentador como por exemplo a ANATEL no Brasil, portanto entendemos que serão aceitos os produtos com homologação ANATEL, além disso o produto ofertado é desenvolvido conforme normativas do IEEE, que regulamenta mundialmente os protocolos de interoperabilidade entre dispositivos wireless e cabeados garantindo assim a interoperabilidade entre equipamentos que implementam os devidos protocolos. Está correto o nosso entendimento?

Resposta: O entendimento não está correto. O certificado de Conectividade Wi-Fi CERTIFIED 6 ™ da WIFI Alliance pode ser requerido por qualquer fornecedor.

---

2. HARDWARE

Texto Original: Deve suportar a utilização de sistema antifurto do tipo Kensington ou similar;

Dúvida: Entendemos que os Access Points de ambientação externa são alocados em locais de difícil acesso com alturas relevantes, portanto entendemos que ofertando equipamentos com os kits de instalação, atende ao ítem sem causar prejuízo ao projeto. Está correto o entendimento?

Resposta: O entendimento não está correto. Todos os equipamentos deverão suportar e deverão ser utilizados os sistemas antifurto do tipo Kensington ou similar.

Texto Original: Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (devendo ser utilizado cabo de segurança com chave ou similar);

Dúvida: Entendemos que os Access Points de ambientação externa são alocados em locais de difícil acesso com alturas relevantes, portanto entendemos que ofertando equipamentos com os kits de instalação, atende ao ítem sem causar prejuízo ao projeto. Está correto o entendimento?

Resposta: O entendimento não está correto. Todos os equipamentos deverão suportar e deverão ser utilizados os sistemas antifurto do tipo Kensington ou similar.

---

4. SEGURANÇA

Texto Original: Deve possuir rádio Bluetooth Low-Energy (BLE);

Sugestão: Retirar ítem - Não faz sentido este recurso sendo que aumenta o consumo e não tem aplicação voltada para a escola usando este tipo de dispositivo, para isso precisaria de um outro projeto já direcionado.

Resposta: A sugestão não será acatada.

Texto Original: Deve implementar recurso de Target Wake Time (TWT);

Sugestão: Retirar ítem direcionado ARUBA - https://www.arubanetworks.com/br/faq/o-que-e-wi-fi-6/

Resposta: A sugestão não será acatada. Target Wake Time (TWT) é um recurso usado em tecnologias de wi-fi 6, sendo utilizado por vários fabricantes.

---

6. INFORMAÇÕES COMPLEMENTARES

Texto Original: Deve implementar recursos de filtro de aplicação para reconhecimento e bloqueio de conteúdos relacionados a jogos,

compartilhamento de arquivos, redes sociais, entre outros. Caso este recurso necessite de licença, a mesma deve ser fornecida pelo mesmo período de tempo coberto pela garantia solicitada neste termo de referência.

Sugestão: Retirar ítem - Missão de segurança deve vir do Firewall nas escolas.

Resposta: A sugestão não será acatada.

Texto Original: Deve implementar a visualização/identificação e marcação das aplicações para permitir o bloqueio ou priorização. Deve permitir a definição de endereços MAC para controle de acesso a rede WiFi.

Sugestão: Retirar ítem - Missão de segurança deve vir do Firewall nas escolas.

Resposta: A sugestão não será acatada.

Texto Original: Operador: acesso de apenas leitura às configurações para a monitoria, sem permissão para alterar configurações; Organizador de Visitantes: acesso e permissão exclusiva para criação de usuários temporários e visitantes para acesso a rede WiFi.

Sugestão: Retirar ítem

Resposta: A sugestão não será acatada.

Texto Original: Deve suportar autenticação de usuários na rede por meio de contas da Google.

Sugestão: Retirar ítem - Direcionamento

Resposta: A sugestão não será acatada.

Texto Original: Fonte de energia: 100-240 V CA, 50 / 60Hz;

Sugestão: Retirar ítem - Não faz mais sentido este tipo de solicitação, deve solicitar POE para os dispositivos.

Resposta: A sugestão será acatada.

ITEM 2 - PONTO DE ACESSO EXTERNO

Texto Original: Deve ser certificado pela WIFI Alliance na subcategoria Enterprise/Service Provider Access Point, Switch/Controller or Router

Dúvida: Entendemos que cada país possui um órgão regulamentador como por exemplo a ANATEL no Brasil, portanto entendemos que serão aceitos os produtos com homologação ANATEL, além disso o produto ofertado é desenvolvido conforme normativas do IEEE, que regulamenta mundialmente os protocolos de interoperabilidade entre dispositivos wireless e cabeados garantindo assim a interoperabilidade entre equipamentos que implementam os devidos protocolos. Está correto o nosso entendimento?

Resposta: O entendimento não está correto. A certificação WIFI Alliance, na subcategoria Enterprise/Service Provider Access Point, Switch/Controller or Router pode ser requerida por qualquer fornecedor.

Texto Original: Deve possuir o certificado de Conectividade Wi-Fi CERTIFIED 6 ™ da WIFI Alliance;

Dúvida: Entendemos que cada país possui um órgão regulamentador como por exemplo a ANATEL no Brasil, portanto entendemos que serão aceitos os produtos com homologação ANATEL, além disso o produto ofertado é desenvolvido conforme normativas do IEEE, que regulamenta mundialmente os protocolos de interoperabilidade entre dispositivos wireless e cabeados garantindo assim a interoperabilidade entre equipamentos que implementam os devidos protocolos. Está correto o nosso entendimento?

Resposta: O entendimento não está correto. O certificado de Conectividade Wi-Fi CERTIFIED 6 ™ da WIFI Alliance pode ser requerido por qualquer fornecedor.

---

2. HARDWARE

Texto Original: Deve suportar a utilização de sistema antifurto do tipo Kensington ou similar;

Dúvida: Entendemos que os Access Points de ambientação externa são alocados em locais de difícil acesso com alturas relevantes, portanto entendemos que ofertando equipamentos com os kits de instalação, atende ao ítem sem causar prejuízo ao projeto. Está correto o entendimento?

Resposta: O entendimento não está correto. Todos os equipamentos deverão suportar e deverão ser utilizados os sistemas antifurto do tipo Kensington ou similar.

---

3. CONEXÃO DE REDE

Texto Original: Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior e uma interface 1G SFP; Suportar VLANs conforme o padrão IEEE 802.1Q;

Dúvida: As portas SFP e elétrica conforme o descritivo, não serão utilizadas de modo simultâneo, portanto, entendemos que poderá ser ofertado na implementação do projeto onde houver necessidade de implementação de fibra óptica a utilização de conversor de mídia, monomodo ou multimodo. Está correto o entendimento?

Resposta: O entendimento não está correto.

---

5. RÁDIO

Texto Original: Deve Suportar no mínimo 512 clientes por rádio (1024 por AP);

Sugestão: Entendemos que para a aplicação deste projeto, suportar uma capacidade de clientes acima de 250 impactará diretamente na performance dos usuários, desta forma entendemos que ofertar um Access Point com capacidade de 250 cliente por AP, atende plenamente esta solicitação. Está correto o nosso entendimento?

Resposta: O valor do item será redimensionado para 256 clientes por rádio (512 por AP).

Texto Original: Deve possuir rádio Bluetooth Low-Energy (BLE);

Sugestão: Retirar ítem

Resposta: A sugestão não será acatada.

Texto Original: Deve implementar recurso de Target Wake Time (TWT);

Sugestão: Retirar ítem

Resposta: A sugestão não será acatada.

Target Wake Time (TWT) é um recurso usado em tecnologias de wi-fi 6, sendo utilizado por vários fabricantes.

Texto Original: Deve possuir antenas direcionais.

Sugestão: Retirar ítem

Resposta: A sugestão não será acatada.

---

6. INFORMAÇÕES COMPLEMENTARES:

Texto Original: Deve implementar recursos de filtro de aplicação para reconhecimento e bloqueio de conteúdos relacionados a jogos, compartilhamento de arquivos, redes sociais, entre outros. Caso este recurso necessite de licença, a mesma deve ser fornecida pelo mesmo período de tempo coberto pela garantia solicitada neste termo de referência.

Sugestão: Retirar ítem

Resposta: A sugestão não será acatada.

Texto Original: Deve implementar a visualização/identificação e marcação das aplicações para permitir o bloqueio ou priorização. Deve permitir a definição de endereços MAC para controle de acesso a rede WiFi.

Sugestão: Retirar ítem

Resposta: A sugestão não será acatada.

Texto Original: Operador: acesso de apenas leitura às configurações para a monitoria, sem permissão para alterar configurações; Organizador de Visitantes: acesso e permissão exclusiva para criação de usuários temporários e visitantes para acesso a rede WiFi.

Sugestão: Retirar ítem

Resposta: A sugestão não será acatada.

Texto Original: Deve suportar autenticação de usuários na rede por meio de contas da Google.

Sugestão: Retirar ítem

Resposta: A sugestão não será acatada.

ITEM 3 - SWITCHES

Texto Original: Jumbo Frame: 10KB;

Sugestão: Entendemos que o padrão para MTBUs do tipo Jumbo frame é de 9 Kb conforme o mercado, portanto entendemos que ofertando switch com suporte de jumbo frame de 9 Kb atende ao certame. Está correto o entendimento?

Resposta: Sim, o entendimento está correto. A especificação será alterada para 9KB

Texto Original: 24 portas RJ45 10/100/1000Mbps (Auto Negociação / Auto MDI / MDIX) e 4 portas SFP 1G com fornecimento de transceiver BASESR; BASE-SR (300-400m);

Sugestão: Observação cotar os gbics

Resposta: A sugestão não será acatada.

Quanto ao que descrevem o item 9.7. SOLUÇÃO DE GERENCIAMENTO:

Texto Original	Sugestão	
9.7.14. Permitir a visualização de eventuais áreas sem cobertura de RF (áreas de sombra);	Entendemos que ofertando solução possibilitando a simulação de cobertura de acordo com a distribuição dos Aps, baseando-se em área e barreiras/interferências no qual áreas de sombra podem ser identificadas atende o item em sua totalidade. Está correto o entendimento?	Resposta: O entendimento está correto.
9.7.20.6. Suportar SSH, HTTP/HTTPS, SSL, Telnet;	O protocolo SSH (security socket shell) é um protocolo de acesso remoto criptografado, mais seguro que o telnet, e amplamente adotado por sistemas operacionais como Windows, Linux e Macos. Portanto, entendemos que ofertando equipamento com suporte à SSH e não ao TELNET atende ao ítem em sua totalidade sem causar prejuízo ao projeto.	Resposta: O entendimento não está correto.
9.7.31. Deve possuir informação sobre possíveis ameaças à rede detectadas pelos sistemas gerenciados;	Esta capacidade relacionada a segurança da rede é mais eficiente quando implementada na rede fixa, podendo controlar o tráfego proveniente da rede cabeada e da rede sem fio. Adotando este conceito, entendemos que esta funcionalidade específica poderá ser considerada opcional e não obrigatória, visando a competição do certame. Estamos corretos em nosso entendimento?	Resposta: O entendimento está correto, o texto será removido.
9.7.32. Deve possibilitar criação de regras de detecção de ameaças e correlacionar todos os dispositivos gerenciados.		Resposta: O entendimento está correto, o texto será removido.

9.8.8.1. Multifator de autenticação OnConnect	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	**Resposta: A especificação será readequada: "9.8.8.1. Multifator de autenticação"**
9.8.9. Recursos do 360 Security Exchange, incluindo servidores de contexto de endpoint locais e ações de servidor de contexto para o host local e XML.	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	**Resposta: A especificação será readequada: "A solução de autenticação deve permitir integração com ferramentas de segurança de terceiros, tipo antivírus, firewall"**
9.8.11. Deve suportar "Single Sign-on" (SSO) através de SAML	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/techdocs/central/2.5.0/content/nms/user-mgmt/saml-profile-conf.htm**	**Resposta: O entendimento não está correto.**
9.8.11.3. Tipo de dispositivo utilizado,	**Entendemos que não faz sentido e está direcionado novamente. Assim acreditamos tirar este tipo de item.**	**Resposta: A sugestão não será acatada.**
9.8.12. Permitir a visualização de todas informações relativas a cada transação/autenticação em uma única tela, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise.	**Entendemos que disponibilizar informações de acesso do cliente conectado, porém em diferentes telas, também atende ao ítem uma vez que todas as informações solicitadas estão contidas. Tornando o certame mais competitivo trazendo maior economia ao projeto.**	**Resposta: A especificação será readequada:** **"9.8.12. Permitir a visualização de todas informações relativas a cada transação/autenticação, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise."**
9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authentication;	**A solução ofertada possui suporte a Radius com protocolo de autenticação. Protocolo este mais amplamente utilizado que TACACS+. Portanto entendemos que oferecendo solução com suporte a Radius, atendemos o certame na sua totalidade. Está correto o entendimento?**	**Resposta: A especificação será readequada:.** **"9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ ou similar e Web Authentication;"**
9.8.16. Deve implementar funcionalidade de classificação automática de dispositivos ("Device profiling"), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	**Resposta: A sugestão será acatada parcialmente e o texto será revisado.** **"9.8.16. Deve suportar expansão de licenciamento para implementar funcionalidade de classificação automática de dispositivos, de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;"**
9.8.17. Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador,		**Resposta: A especificação será readequada:** **9.8.17. "Deve suportar expansão de**

Smartdevice, impressora, etc.), por sistema operacional (ex. Windows, Linux, MacOS, etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server, etc);	Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf	licenciamento para categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.), por sistema operacional
9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, Active Sync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting;	Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf	Resposta: A especificação será readequada: "9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, SNMP e base de assinaturas;"
9.8.21. Deve implementar os serviços de autenticação, profiling e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos.	Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf	Resposta: A especificação será readequada: "Deve implementar os serviços de autenticação e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos, simultaneamente."
9.8.24. Suporte a RADIUS CoA, Web authentication e SAML v2.0	Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf	Resposta: A sugestão não será acatada Caso a CONTRATADA esteja ofertando solução de gerenciamento que não possua os recursos de autenticação do item 9.8. A mesma poderá ofertar solução integrada, de terceiros, apresentando comprovação de integração entre as soluções de gerenciamento e autenticação.
9.8.25.1. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)	?	Resposta: O item será removido
9.8.25.2. PEAP (EAP-MSCHAPv2, EAP-GTC,EAP-TLS,EAP-PEAP-Public, EAP-PWD)	?	Resposta: O item será mantido
9.8.25.3. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)	?	Resposta:.O item será mantido
9.8.25.4. EAP-TLS	?	Resposta: O item será removido
9.8.25.5. PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5	?	Resposta: O item será removido
9.8.25.7. SMB v2/v3	Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf	Resposta: O item será removido
9.8.25.9. RADSec	Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf	Resposta: O item será removido
9.8.25.10.Online Certificate Status Protocol (OCSP)	Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf	Resposta: O item será removido
	A solução ofertada possui suporte a Radius com protocolo de autenticação.	Resposta: O

9.8.25.11.TACACS+	**Protocolo este mais amplamente utilizado que TACACS+. Portanto entendemos que oferecendo solução com suporte a Radius, atendemos o certame na sua totalidade. Está correto o entendimento?**	**Resposta: O entendimento não está correto.**
9.8.26.Deve suportar a verificação de vulnerabilidade através de varredura de portas (NMAP).	**Esta capacidade relacionada a segurança da rede é mais eficiente quando implementada na rede fixa, podendo controlar o tráfego proveniente da rede cabeada e da rede sem fio. Adotando este conceito, entendemos que esta funcionalidade específica poderá ser considerada opcional e não obrigatória, visando a competição do certame. Estamos corretos em nosso entendimento?**	**Resposta: O entendimento não está correto.**
9.8.28.Permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informações a serem utilizadas durante o processo de autenticação dos usuários.	**A solução ofertada possui suporte a Radius com protocolo de autenticação. Protocolo este mais amplamente utilizado que bases SQL. Portanto entendemos que oferecendo solução com suporte a Radius, atendemos o certame na sua totalidade. Está correto o entendimento?**	**Resposta: O entendimento não está correto.**
9.8.29.Suporte aos seguintes recursos através de IPv6:	**Todos os protocolos solicitados para ipv6 são de finalidade de gerenciamento, no qual são normalmente disponibilizados em infraestrutura interna ou serviço em nuvem. O protocolo ipv6 é amplamente adotado para a rede mundial de computadores (internet) onde não há mais endereçamentos ipv4 disponíveis, porém para redes internas em sua totalidade o protocolo ipv4 são mais amplamente adotados portanto entendendo que ofertando soluções de gerenciamento em ipv4 atende ao ítem em sua totalidade. Estamos corretos em nosso questionamento?**	**Resposta: O entendimento não está correto.** **Resposta: A especificação será readequada:** **"9.8.29. Suporte a servidores de autenticação e autorização com endereçamento IPv6;** **9.8.29.1. Fontes de Syslog para processamento de evento"**
9.8.29.1.Administração via WEB e CLI	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.2. Servidores de autenticação e autorização com endereçamento IPv6;	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.3. IPv6 Accounting Proxy;	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.4. Acesso a servidores com endereçamento IPv6 para contexto de endpoints;	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.5. Syslog, DNS, NTP;	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.6. Endereçamento IPv6 para VIP (Virtual IP) de alta disponibilidade;	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.7. Fontes de Syslog para processamento de evento	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.8. Validações e conformidades: 9.8.29.8.1. FIPS 140-2	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.29.8.2. Common Criteria NDcPP+Servidor de autenticação	**Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf**	
9.8.30. A solução deve permitir configuração em alta disponibilidade com no mínimo dois elementos, sendo que ambos devem permanecer ativos para o processamento das requisições;	**Quando solicitado configuração em alta disponibilidade entendemos que está sendo solicitado appliance, entretanto, visando maior competitividade entendemos que ofertando solução com possibilidade de servidor virtualizado no qual possui nativamente estratégias de redundância, bem como nuvem atende ao ítem em sua totalidade sem causar prejuízo ao projeto.**	**Resposta: A sugestão não será acatada Caso a CONTRATADA esteja ofertando solução de gerenciamento que não possua os recursos de autenticação do item 9.8. A mesma poderá ofertar solução integrada, de terceiros, apresentando comprovação de integração entre as soluções de gerenciamento e**

		autenticação.
9.8.33. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML e PDF.	Entendemos que entregando relatórios de forma manual, atende ao ítem, tornando o certame mais competitivo trazendo maior economia ao projeto.	Resposta: O entendimento não está correto. A especificação será readequada: 9.8.33. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML ou CSV ou EXCEL e PDF.
9.8.34. A solução deve ter suporte do fabricante no horário de 08:00h às 20:00h de segunda a sexta feira, durante todo o período de contrato.	Entendemos que o atendimento do suporte técnico pode ser realizado por parceiros credenciados e autorizados pelo fabricante conforme horários solicitados. Está correto o entendimento?	Resposta: O entendimento está correto.
9.8.29.2. Servidores de autenticação e autorização com endereçamento IPv6;	Entendemos que não pode haver direcionamento para fabricante, Assim acreditamos que este item seja retirado, totalmente escrito para Aruba! https://www.arubanetworks.com/assets/_pt-br/so/SO_MFP.pdf	Resposta: O entendimento está correto.

ITEM 5 - NOBREAK

Texto Original	Sugestão	
Fator de potência: 0,7;	Solicitamos que seja modificado para 0,5 , permitindo assim outros participarem com indústria nacional. Essa alteração irá permitir às empresas com fabricação local o fornecimento do item aumentando assim as possibilidades de mais opções de compra.	Resposta: Não será acatado
Frequência de entrada: 50/60 HZ;	Mudar frequencia 60 HZ padrão Brasil. Essa alteração irá permitir às empresas com fabricação local o fornecimento do item aumentando assim as possibilidades de mais opções de compra.	Resposta:Não será acatado
Tipo de Tomada: mínimo 6 Tomadas/Bornes padrão NBR 14.136;	Solicitamos que seja modificado para 04 , permitindo assim outros participarem com indústria nacional. Localidade que precisarem de mais tomas usa-se régua para estender, senão tudo liga no nobreak e pode comprometer. Essa alteração irá permitir às empresas com fabricação local o fornecimento do item aumentando assim as possibilidades de mais opções de compra.	Resposta:Não será acatado
Possuir porta fusível externo que acomoda uma unidade reserva;	Mudar para Possuir porta fusível externo , retirar que acomode uma unidade reserva.. Direcionamento.Essa alteração irá permitir às empresas com fabricação local o fornecimento do item aumentando assim as possibilidades de mais opções de compra.	Resposta:Não será acatado
Possuir a função Autoteste, pois ao ser ligado realizará os testes dos circuitos internos e das baterias;	Retirar, pois direciona, nobreak deve ter luz indicativa de uso da bateria por falta de energia. Essa alteração irá permitir às empresas com fabricação local o fornecimento do item aumentando assim as possibilidades de mais opções de compra.	Resposta:Não será acatado

Nobreak direcionado:

https://proups.com.br/produto/view/varios-modelos-station-ii-600-800-e-1200-va#.YzRcTnbMLIU

Resposta: Não foi confirmado o direcionamento para o equipamento nobreak, tendo em vista que diversos fabricantes atendem às especificações do item presentes no Termo de Referência

---

HUAWEI

1. CONSIDERAÇÕES GERAIS

Texto Original: 1.2.5. Todos os produtos em hardware, software e licenças de um grupo devem ser de um único fabricante, de modo a garantir plena compatibilidade.

Sugestão de Alteração: 1.2.5. Todos os produtos em hardware, software e licenças de um grupo devem ser de um único fabricante, exceto os itens 4 – Rack e 5 – Nobreak, de modo a garantir plena compatibilidade.

Justificativa: Solicitamos que os itens 4 – Rack e 5 – Nobreak possam ser de fabricantes diversos ao da solução de WLAN e LAN, já que esses itens são suplantares e não integráveis à gerência da solução principal. A Huawei comercializa no mercado brasileiro a linha de UPS (Uninterruptible Power Supply, comumente chamado de Nobreak), entretanto disponibiliza apenas equipamentos robustos para ambientes de datacenter. Diversos outros fabricantes não possuem o equipamento Nobreak em suas linhas comerciais. Os racks são comercializados pelos fabricantes, mas, assim como o Nobreak, é solicitado em característica simples e de pequeno porte, sendo a composição da solução com fabricantes especializados de Rack e Nobreak mais vantajosa financeiramente à administração pública, os quais terão equipamentos adequados para o porte solicitado, sem prejuízos ao bom funcionamento da solução de WLAN e LAN para as escolas de MG.

Resposta: A sugestão será acatada.

Adicionar: Os equipamentos sujeitos à homologação na ANATEL devem possuir certificado válido na entrega do equipamento.

Justificativa: Solicitamos adicionar (sugestão: no tópico: "7. CRITÉRIOS DE ACEITABILIDADE DA PROPOSTA")

condição para apresentação da homologação da ANATEL para todos os itens sujeitos ao processo de

homologação no momento da entrega dos equipamentos.

Resposta: Resposta: A sugestão não será acatada. Pois de acordo com subitem 7.6: Serão avaliados os aspectos e padrões mínimos de aceitabilidade conforme ANEXO A - ESPECIFICAÇÕES TÉCNICAS.

Texto Original:

7.3. Caso a compatibilidade com as especificações demandadas, sobretudo quanto a padrões de qualidade e desempenho, não possa ser aferida pelos meios previstos no subitem acima, o Pregoeiro exigirá que o licitante classificado em primeiro lugar apresente amostra, sob pena de não aceitação da proposta, no local a ser indicado e dentro de 5 (cinco) dias úteis contados da solicitação.

7.7. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

Sugestão de Alteração:

7.3. Caso a compatibilidade com as especificações demandadas, sobretudo quanto a padrões de qualidade e desempenho, não possa ser aferida pelos meios previstos no subitem acima, o Pregoeiro exigirá demonstração do recurso a ser aferido dentro de 5 (cinco) dias úteis contados da solicitação. A demonstração deve ser realizada preferencialmente de forma remota, também sendo aceita demonstração com amostra local.

7.7. No caso de não haver a demonstração exigida, sem justificativa aceita pelo Pregoeiro, ou sendo constatado que a demonstração das especificações previstas neste Edital, a proposta do licitante será recusada.

Justificativa: Solicitamos que, no caso das especificações demandadas não possam ser verificadas pela documentação fornecida, seja solicitado teste remoto de forma preferencial em alternativa à entrega de amostras locais. O teste remoto assegura as condições de teste, eliminando a possibilidade do fornecedor afirmar falhas no cenário preparado pelo cliente para os testes. O teste remoto ainda pode ser realizado de forma mais célere, sem atrasos no processo para a entrega de equipamento de amostra.

Resposta: A sugestão não será acatada, pois o texto não exclui a possibilidade da demonstração ser realizada de forma remota

---

CONSIDERAÇÕES TÉCNICAS

1. PONTO DE ACESSO INTERNO

Texto Original: Possuir capacidade de montagem em parede e teto, devendo ser fornecidos todos os acessórios necessários para estas montagens;

Sugestão de Alteração: Possuir capacidade de montagem em parede e teto, devendo ser fornecidos todos os acessórios necessários para estas montagens, devendo ser do mesmo fabricante do ponto de acesso.

Justificativa: Com o objetivo de assegurar total compatibilidade dos acessórios fornecidos, eliminando chances de soluções improvisadas que possam interferir no melhor funcionamento das antenas, sugerimos que os acessórios de montagem sejam obrigatoriamente do mesmo fabricante dos APs.

Resposta: A sugestão não será acatada.

Texto Original: Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c ou SNMPv3, incluindo a geração de traps;

Sugestão de Alteração: Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps, ou NETCONF.

Justificativa: A primeira parte da sugestão tem como objetivo assegurar a implementação do SNMPv3, assim como é solicitado no software de gerenciamento item "9.7.22.". O SNMPv3 fornece todas as funções do SNMPv1 e SNMPv2, e apresenta um mecanismo de segurança que autentica e criptografa pacotes SNMP. Em termos de segurança, o SNMPv3 enfatiza a segurança dos dados e o controle de acesso. O SNMPv3 garante a segurança dos pacotes SNMP das seguintes maneiras:

1. Verificação da integridade dos dados Os dados não podem ser modificados de forma não autorizada. A alteração da sequência de dados é limitada à extensão permitida.

2. Autenticação de origem de dados O SNMPv3 autentica o nó gerenciado do qual a origem é recebida e não o aplicativo que gera o pacote.

3. Confidencialidade dos dados: Quando o NMS ou o agente recebem um pacote, verificam a hora em que o pacote é gerado. Se a diferença entre a hora de criação e a hora do sistema exceder o limite, o pacote será descartado. Desta forma, os pacotes que são modificados por mal-intencionados não são aceitos.

A segunda parte da sugestão é a adição de uma alternativa de protocolo de gerenciamento. A sugestão apenas acrescenta uma alternativa, não altera para os fabricantes que implementam a gerência por meio de SNMP. O NETCONF, assim como o SNMP, é um protocolo aberto e inclusive mais interoperável que o SNMP.

O Network Configuration Protocol (NETCONF) é um protocolo de gerenciamento de rede que permite que um sistema de gerenciamento de rede (NMS) entregue, modifique e exclua configurações de dispositivos de rede.

As interfaces de programação de aplicativos (APIs) padrão estão disponíveis em dispositivos de rede para que o NMS gerencie os dispositivos usando o NETCONF. Para superar as desvantagens da CLI e do SNMP, o

NETCONF baseado em XML é introduzido, que tem as seguintes vantagens:

1. NETCONF usa uma estrutura de protocolo hierárquico, tornando-o mais adequado para requisitos de big data, automatizados e sob demanda de redes baseadas em nuvem.

2. NETCONF usa codificação XML para definir mensagens e usa o mecanismo RPC para modificar dados de configuração. Isso facilita o gerenciamento de dados de configuração e a interoperabilidade entre dispositivos de diferentes fornecedores.

3. O NETCONF realiza operações em dispositivos baseados no modelo YANG, reduzindo falhas de rede causadas por erros de configuração manual.

4. NETCONF fornece mecanismos de segurança, como autenticação e autorização para garantir a segurança da transmissão de mensagens.

5. O NETCONF fornece um mecanismo de transação para oferecer suporte à classificação, armazenamento e migração de dados, envio baseado em fases, isolamento de configuração, bem como entrega, verificação e reversão de configuração geral, minimizando o impacto nos serviços de

rede.

Resposta: A sugestão será acatada parcialmente:

“Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c ou SNMPv3, incluindo a geração de traps e/ ou NETCONF”

Texto Original: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 e SAE-AES;

Sugestão de Alteração: Implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal.

Justificativa: Solicitamos a alteração para termos utilizados pela Wi-Fi Alliance (https://www.wi-fi.org/discover-wi-fi/security) para definir os padrões de segurança WPA3. O texto sugerido possibilita a fácil compreensão e identificação ao atendimento de diversos fabricantes e engloba os modos de criptografia de 128, 192 e 256 bits.

Resposta: A sugestão será atendida parcialmente:

“Poderá ser implementado WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES ou, ainda, implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal.”

Texto Original: Possuir antenas internas com ganho mínimo de 2,5dBi em 2,4GHz e 3 dBi em 5GHz;

Sugestão de Alteração: Possuir antenas internas com ganho mínimo de 2dBi em 2,4GHz e 3 dBi em 5GHz;

Justificativa: Solicitamos alteração de ganho em 2.4GHz de 2,5 para 2 dBi. A pequena alteração não afeta no funcionamento da solução e limita a participação de fabricantes com equipamentos adequados ao porte das escolas.

Resposta: A sugestão será acatada:

Possuir antenas internas com ganho mínimo de 2dBi em 2,4GHz e 3 dBi em 5GHz;

Texto Original: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem.

Sugestão de Alteração: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem em infra-estrutura privada e de uso exclusivo da Secretaria de Estado de Educação de Minas Gerais.

Justificativa: Sugestão para clarificar o modo de implementação da controladora/gerência. O texto “nuvem” pode ser interpretado como nuvem pública. Apesar de já estar descrito no software de gerenciamento que a solução deve estar instalada em infra-estrutura da contratada para ser posteriormente migrada para a infra-estrutura da contratante, a descrição pode ser mais clara nos APs para não restar dúvidas que não serão aceitas soluções em nuvem pública.

Resposta: A sugestão não será acatada

Texto Original: Deve incluir solução de controladora em nuvem responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários.

Sugestão de Alteração: Deve incluir solução de controladora em nuvem em infra-estrutura privada e de uso exclusivo da Secretaria de Estado de Educação de Minas Gerais responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de

dispositivos de usuários.

Justificativa: Sugestão para clarificar o modo de implementação da controladora/gerência. O texto "nuvem" pode ser interpretado como nuvem pública. Apesar de já estar descrito no software de gerenciamento que a solução deve estar instalada em infra-estrutura da contratada para ser posteriormente migrada para a infra-estrutura da contratante, a descrição pode ser mais clara nos APs para não restar dúvidas que não serão aceitas soluções em nuvem pública.

Resposta: A sugestão não será acatada

Texto Original: A solução de Controladora Wireless em Nuvem deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração.

Sugestão de Alteração: A solução de Controladora Wireless em Nuvem em infra-estrutura privada e de uso exclusivo da Secretaria de Estado de Educação de Minas Gerais deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de

Referência em um mesmo console de administração.

Justificativa: Sugestão para clarificar o modo de implementação da controladora/gerência. O texto "nuvem" pode ser interpretado como nuvem pública. Apesar de já estar descrito no software de gerenciamento que a solução deve estar instalada em infra-estrutura da contratada para ser posteriormente migrada para a infra-estrutura da contratante, a descrição pode ser mais clara nos APs para não restar dúvidas que não serão aceitas soluções em nuvem pública.

Resposta: A sugestão não será acatada

---

2. PONTO DE ACESSO EXTERNO

Texto Original: Possuir capacidade de montagem em parede e teto, devendo ser fornecidos todos os acessórios necessários para estas montagens;

Sugestão de Alteração: Possuir capacidade de montagem em parede e teto, devendo ser fornecidos todos os acessórios necessários para estas montagens, devendo ser do mesmo fabricante do ponto de acesso.

Justificativa: Com o objetivo de assegurar total compatibilidade dos acessórios fornecidos, eliminando chances de soluções improvisadas que possam interferir no melhor funcionamento das antenas, sugerimos que os acessórios de montagem sejam obrigatoriamente do mesmo fabricante dos APs.

Resposta: A sugestão não será acatada.

Texto Original: Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior e uma interface 1G SFP;

Sugestão de Alteração: Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior e uma interface 1G SFP. Deve vir com fornecimento de 1 transceiver BASESR; BASE-SR (300-400m).

Justificativa: Sugerimos solicitar o transceiver necessário para a utilização da porta óptica do AP externo.

Resposta: A especificação será readequada.

"Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior e uma interface 1G SFP. Deve ser fornecido transceiver, caso o modelo não suporte conexão direta da fibra BASESR; BASE-SR (300-400m)."

Texto Original: Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c ou SNMPv3, incluindo a geração de traps;

Sugestão de Alteração: Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps, ou NETCONF.

Justificativa: A primeira parte da sugestão tem como objetivo assegurar a implementação do SNMPv3, assim como é solicitado no software de gerenciamento item "9.7.22.". O SNMPv3 fornece todas as funções do SNMPv1 e SNMPv2, e apresenta um mecanismo de segurança que autentica e criptografa pacotes SNMP. Em termos de segurança, o SNMPv3 enfatiza a segurança dos dados e o controle de acesso. O SNMPv3 garante a segurança dos pacotes SNMP das seguintes maneiras:

1. Verificação da integridade dos dados Os dados não podem ser modificados de forma não autorizada. A alteração da sequência de dados é limitada à extensão permitida.

2. Autenticação de origem de dados O SNMPv3 autentica o nó gerenciado do qual a origem é recebida e não o aplicativo que gera o pacote.

3. Confidencialidade dos dados: Quando o NMS ou o agente recebe um pacote, verificam a hora em que o pacote é gerado. Se a diferença entre a hora de criação e a hora do sistema exceder o limite, o pacote será descartado. Desta forma, os pacotes que são modificados por mal-intencionados não são aceitos.

A segunda parte da sugestão é a adição de uma alternativa de protocolo de gerenciamento. A sugestão apenas acrescenta uma alternativa, não altera para os fabricantes que implementam a gerência por meio de SNMP. O NETCONF, assim como o SNMP, é um protocolo aberto e inclusive mais interoperável que o SNMP.

O Network Configuration Protocol (NETCONF) é um protocolo de gerenciamento de rede que permite que um sistema de gerenciamento de rede (NMS) entregue, modifique e exclua configurações de dispositivos de rede.

As interfaces de programação de aplicativos (APIs) padrão estão disponíveis em dispositivos de rede para que o NMS gerencie os dispositivos usando o NETCONF. Para superar as desvantagens da CLI e do SNMP, o

NETCONF baseado em XML é introduzido, que tem as seguintes vantagens:

1. NETCONF usa uma estrutura de protocolo hierárquico, tornando-o mais adequado para requisitos de big data, automatizados e sob demanda de redes baseadas em nuvem.

2. NETCONF usa codificação XML para definir mensagens e usa o mecanismo RPC para modificar dados de configuração. Isso facilita o gerenciamento de dados de configuração e a interoperabilidade entre dispositivos de diferentes fornecedores.

3. O NETCONF realiza operações em dispositivos baseados no modelo YANG, reduzindo falhas de rede causadas por erros de configuração manual.

4. NETCONF fornece mecanismos de segurança, como autenticação e autorização para garantir a segurança da transmissão de mensagens.

5. O NETCONF fornece um mecanismo de transação para oferecer suporte à classificação, armazenamento e migração de dados, envio baseado em fases, isolamento de configuração, bem como entrega, verificação e reversão de configuração geral, minimizando o impacto nos serviços de rede.

Resposta: A sugestão será acatada parcialmente:

"Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c ou SNMPv3, incluindo a geração de traps e/ ou NETCONF"

Texto Original: Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 e SAE-AES;

Sugestão de Alteração: Implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal.

Justificativa: Solicitamos a alteração para termos utilizados pela Wi-Fi Alliance (https://www.wi-fi.org/discover-wi-fi/security) para definir os padrões de segurança WPA3. O texto sugerido possibilita a fácil compreensão e identificação ao atendimento de diversos fabricantes e engloba os modos de criptografia de 128, 192 e 256 bits.

Resposta: A sugestão será atendida parcialmente:

"Poderá ser implementado WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 ou AES-GCM-256 e SAE-AES ou, ainda, implementar WPA3 com algoritmo de criptografia WPA3-Enterprise 192-bit e WPA3-Personal."

Texto Original: Deve possuir captive portal web (HTTPS) de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem.

Sugestão de Alteração: Deve possuir captive portal web (HTTPS) de

autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem em infra-estrutura privada e de uso exclusivo da Secretaria de Estado de Educação de Minas Gerais.

Justificativa: Sugestão para clarificar o modo de implementação da controladora/gerência. O texto "nuvem" pode ser interpretado como nuvem pública. Apesar de já estar descrito no software de gerenciamento que a solução deve estar instalada em infra-estrutura da contratada para ser posteriormente migrada para a infra-estrutura da contratante, a descrição pode ser mais clara nos APs para não restar dúvidas que não serão aceitas soluções em nuvem pública.

Resposta: A sugestão não será acatada

Texto Original: Deve incluir solução de controladora em nuvem responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários.

Sugestão de Alteração: Deve incluir solução de controladora em nuvem em infra-estrutura privada e de uso exclusivo da Secretaria de Estado de Educação de Minas Gerais responsável pelas seguintes funções na rede sem fio: Administração; Configuração; e Gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de gerenciamento de RF (Radiofrequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários.

Justificativa: Sugestão para clarificar o modo de implementação da controladora/gerência. O texto "nuvem" pode ser interpretado como nuvem pública. Apesar de já estar descrito no software de gerenciamento que a solução deve estar instalada em infra-estrutura da contratada para ser posteriormente migrada para a infra-estrutura da contratante, a descrição pode ser mais clara nos APs para não restar dúvidas que não serão aceitas soluções em nuvem pública.

Resposta: A sugestão não será acatada

Texto Original: A solução de Controladora Wireless em Nuvem deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de Referência em uma mesma console de administração.

Sugestão de Alteração: A solução de Controladora Wireless em Nuvem em infra-estrutura privada e de uso exclusivo da Secretaria de Estado de Educação de Minas Gerais deve possuir uptime (disponibilidade) de 99,6% ao ano. A solução deve suportar a quantidade total de Pontos de Acessos descritos neste Termo de

Referência em um mesmo console de administração.

Justificativa: Sugestão para clarificar o modo de implementação da controladora/gerência. O texto "nuvem" pode ser interpretado como nuvem pública. Apesar de já estar descrito no software de gerenciamento que a solução deve estar instalada em infra-estrutura da contratada para ser posteriormente migrada para a infra-estrutura da contratante, a descrição pode ser mais clara nos APs para não restar dúvidas que não serão aceitas soluções em nuvem pública.

Resposta: A sugestão não será acatada

Texto Original: Fonte de energia: 100-240 V CA, 50 / 60Hz; FCC, CE, RoHS.

Sugestão de Alteração: Fonte de energia: 100-240 V CA, 50 / 60Hz; FCC, CE, RoHS. Ou injetor PoE adequado para o funcionamento do ponto de acesso externo

Justificativa: Solicitamos a alteração, sem prejuízos ao funcionamento da solução. O injetor PoE funcionará exatamente como uma fonte de alimentação para o ponto de acesso externo. Devido ao AP de ambientes externos da Huawei possuir o maior nível de proteção contra intempéries do mercado, o IP68, o AP não possui abertura desprotegida para fonte de energia. A porta de rede em que o cabo de alimentação PoE (por meio do switch PoE ou injetor PoE) é conectado é totalmente protegida contra água e poeira.

Resposta: A sugestão não será acatada

---

3. SWITCHES

Remover o item: Auto Uplink em Cada Porta;

Justificativa: Solicitamos que o item seja removido. Em razão do termo "Auto Uplink" ser específico de um fabricante (TP-LINK), há dúvidas sobre a funcionalidade requerida. Não foram encontradas explicações profundas do fabricante sobre o que essa funcionalidade trata. Não é recomendado ter especificações que dependem de interpretação. No nosso entendimento, o termo é relacionada à funcionalidade de auto-negociação, em que as portas do switch negociam a velocidade automaticamente, já solicitada no item "24 portas RJ45 10/100/1000Mbps (Auto Negociação / Auto MDI / MDIX) e 4 portas SFP 1G com fornecimento de transceiver BASESR; BASE-SR (300-400m);"

Resposta: A sugestão será acatada

Texto Original: Controle de Fluxo 802.3x, Back;

Sugestão de Alteração: Controle de Fluxo 802.3x.

Resposta: A sugestão será acatada

Texto Original: Comutação: 52 Gbps;

Sugestão de Alteração: Comutação: 56 Gbps

Justificativa: É solicitado switch de 24 portas 1G BASE-T UTP mais 4 portas 1G SFP. Para o switch ser non-blocking, ou seja, ser capaz de comutar toda comunicação de todas as portas simultaneamente em suas capacidades máximas, deve realizar comutação de 24 + 4 = 28 Gbps. Considerando a comunicação bidirecional (full-duplex), deve ter capacidade de 28 x 2 = 56 Gbps.

Resposta: Resposta: A sugestão será acatada parcialmente:

Comutação: mínimo de 52 Gbps;

Texto Original: Taxa de encaminhamento de pacotes: 36Mpps;

Sugestão de Alteração: Taxa de encaminhamento de pacotes: 42Mbps;

Justificativa: É solicitado switch de 24 portas 1G BASE-T UTP mais 4 portas 1G SFP. Para o switch ser wire-speed, ou seja, ser capaz de encaminhar todo o tráfego de todas as portas simultaneamente em suas capacidades máximas, deve possuir taxa de encaminhamento de pacotes de (28 Gbps / 8) / 84 bytes = 41.6 Mpps. A lógica do cálculo é dada por: primeiramente dividir a banda unidirecional das portas presentes por 8 para se ter o número em gigabytes por segundo, seguida da divisão pela quantidade de bytes do menor pacote possível (64 bytes de dataframe + 8 bytes de preâmbulo + 12 bytes de interframe gap = 84 bytes), obtendo o resultado em milhões de pacotes por segundo.

Resposta: A especificação será readequada:

"Taxa de encaminhamento de pacotes: mínimo de 36 Mpps;"

Texto Original: Jumbo Frame: 10KB;

Sugestão de Alteração: Jumbo Frame: 9KB;

Justificativa: Solicitamos alteração de Jumbo Frames para 9KB. A pequena alteração não afetará no funcionamento da solução e limita a participação de fabricantes com equipamentos adequados ao porte das escolas.

Resposta: A sugestão será acatada, será alterada para 9KB.

Texto Original: 24 portas RJ45 10/100/1000Mbps (Auto Negociação /Auto MDI / MDIX) e 4 portas SFP 1G com fornecimento de transceiver BASESR; BASE-SR (300-400m);

Sugestão de Alteração: 24 portas RJ45 10/100/1000Mbps (Auto

Negociação /Auto MDI / MDIX) e 4 portas SFP 1G populadas com transceivers BASESR; BASE-SR (300-400m); Ou

24 portas RJ45 10/100/1000Mbps (Auto Negociação /Auto MDI / MDIX) e 4 portas SFP 1G com fornecimento de 1 transceiver BASESR; BASE-SR (300-400m) por switch;

Justificativa: Sugerimos a descrição mais clara de quantos transceivers devem ser fornecidos por switch.

Resposta: A especificação será readequada:

24 portas RJ45 10/100/1000Mbps (Auto Negociação/ Auto MDI/ MDIX) e 4 portas SFP 1G com fornecimento de transceivers BASESR; BASE-SR (300-400m) 1 para switch e 1 para ponto de acesso externo.

Texto Original: Implementar o padrão PoE em todas as 24 portas RJ-45, com potência energética necessária nas portas PoE a fim de atender na plenitude o funcionamento dos AP`s;

Sugestão de Alteração: Implementar o padrão PoE em todas as 24 portas RJ-45, com potência energética necessária nas portas PoE a fim de atender simultaneamente todas as 24 portas do switch em 802.3af. A potência PoE entregue pelo switch deve atender no mínimo 10 APs internos e 1 AP externo.

Justificativa: Sugerimos que seja solicitado no mínimo o funcionamento simultâneo de todas as 24 portas em 15.4 W (802.3af), para efeito de preservação de investimento, o equipamento pode servir para alimentar câmeras ou outros dispositivos PoE, sendo uma característica básica dos switches de entrada dos mais diversos fabricantes.

Ainda, deve ser assegurado que o switch atenda à potência necessária para os APs, caso ultrapasse o total previsto sugerido (15.4W x 24 = 370W). A potência de PoE para atender na plenitude o funcionamento dos AP's é dependente da quantidade de APs que serão alimentados, por exemplo, supondo que os APs internos e externos ofertados por determinado fabricante possuam especificação de consumo máximo de 15W (padrão 802.3af) e 30W (padrão 802.3at), respectivamente. Para alimentar 5 APs internos e 1 AP externo são necessários 105W de potência de PoE no switch. Caso os APs ofertados utilizem maior potência de alimentação, a lógica do cálculo é a mesma e pode ultrapassar os 370W previstos. Para o participante do certame fazer o cálculo corretamente, é necessário indicar as quantidades de APs, sendo assim, sugerimos a

alteração para clarificar a quantidade máxima de APs prevista em cada switch.

Resposta: A sugestão não será acatada

Sugestão de Adição: Implementar 2000 VLANs ativas/ Implementar 2000 ACLs ativas.

Justificativa: A implementação de VLANs e ACLs no switch são características básicas para a implementação de redes seguras e controladas nas escolas. A sugestão é baseada nas melhores práticas elaboradas por décadas de experiência da Huawei. O objetivo principal do projeto é prover cobertura wireless de qualidade para todas as escolas, um recurso poderoso para fugir do controle da SEE ou ser implementado sem a devida preocupação com segurança.

Nas escolas temos o acesso de estudantes, professores, profissionais administrativos, profissionais comuns (ex. limpeza e manutenção), visitantes (ex: pais e eventos), etc. Normalmente essas redes são separadas em

diferentes SSIDs, mas, para segmentar de fato a rede desses diversos usuários, é necessário associar cada SSID a uma VLAN diferente. Ainda, é recomendado segmentar a rede de endpoints como câmeras, como premissa básica de segurança, já que as credenciais desses endpoints podem ser facilmente quebradas, e na ocasião da implementação de uma rede única, a invasão à rede pode facilmente se estender a todos os equipamentos conectados, incluindo computadores administrativos e de professores. A implementação de ACL assegura a utilização dos recursos da rede aos devidos usuários privilegiados e autenticados, também contribuindo para a segurança da rede.

Os valores solicitados são pequenos, os equipamentos Huawei implementam muito mais recursos de VLAN e de ACL. A sugestão visa assegurar a qualidade da implementação do projeto, independente do vencedor do certame.

Resposta: A sugestão não será acatada

9.7 - SOLUÇÃO DE GERENCIAMENTO

Texto Original:

9.7.1. Os equipamentos devem incluir Solução de Gerência da Rede Sem Fio deve ser fornecida em Appliance Virtual;

9.7.8. A solução deverá ser disponibilizada através da imagem de sistema operacional, já com os softwares necessários para a instalação em VMWARE.

Sugestão de Alteração: Substituir os itens 9.7.1 e 9.7.8 por:

9.7.8. Deverão ser providos quantos softwares e ou appliance forem necessários para realizar as funções

de gerenciamento e controle de todos os pontos de acesso e switches contratados, incluindo sistema operacional e todas as licenças necessárias.

Justificativa: A solução ofertada deve incluir os appliances, softwares, sistema operacional e sistemas de virtualização necessários ao funcionamento da solução, não havendo motivos para limitar o tipo de Hypersor utilizado. Dessa forma, solicitamos a alteração para que todos os recursos para o funcionamento pleno da solução sejam entregues, de acordo com as especificações dos diferentes fabricantes.

Resposta: A especificação do subitem 9.7.8. será readequada:

"9.7.8. A solução deverá ser disponibilizada através da imagem de sistema operacional, já com os softwares e licenças necessárias para a instalação em VMWARE."

Texto Original: 9.7.4. A solução deve suportar e estar licenciado para gerenciar todos os APs E switches constantes neste termo de referência;

Sugestão de Alteração: 9.7.4. A solução deve suportar gerenciar todos os APs E switches constantes neste termo de referência;

Justificativa: O item original é ligeiramente contraditório com o item seguinte "9.7.5. Deve ser licenciado em quantidade unitária, sendo uma licença por dispositivo a ser gerenciado.". Financeiramente é mais vantajoso para o cliente o licenciamento unitário, uma vez que trata-se de uma ATA de registro de preço, em que as aquisições são feitas em partes. Não é vantajoso pagar pelo software de gerenciamento licenciado para a quantidade total de equipamentos sem ter a certeza de aquisição dessa quantidade de equipamentos (APs e switches). Assim, sugerimos a alteração no item para reforçar o licenciamento unitário, já solicitado no item 9.7.5.

A sugestão será desconsiderada, pois não existem discrepâncias entre o texto original e a sugestão.

Texto Original: 9.7.7. A solução deve estar instalada em infraestrutura da CONTRATADA podendo ser migrado para infraestrutura da CONTRATANTE no término do contrato ou quando for solicitado.

Sugestão de Alteração: 9.7.7. A solução deve estar instalada em infraestrutura sob responsabilidade da CONTRATADA podendo ser migrado para infraestrutura da CONTRATANTE no término do contrato ou quando for solicitado.

Justificativa: Sugerimos a alteração para a possibilidade da contratação de ambientes de ISPs para implementação da infra-estrutura, com o fornecimento de ambiente especializado para os equipamentos.

Resposta: A sugestão não será acatada

Texto Original: 9.7.2. Deve ser obrigatoriamente do mesmo fabricante dos pontos de acesso;

Sugestão de Alteração: 9.7.2. Deve ser obrigatoriamente do mesmo fabricante dos pontos de acesso e dos switches

Justificativa: Sugerimos a utilização de uma solução unificada e centralizada dos ativos (APs e switches) do projeto.

Resposta: A sugestão não será acatada

Texto Original:

9.7.11. Possuir capacidade de projeto automatizado de redes sem fio nos

padrões 802.11a, 802.11b e 802.11g, 802.11n, 802.11ac e 802.11ax, segundo a geografia do prédio;

9.7.12. Considerar a área de cobertura e a banda por usuário desejada;

9.7.14. Permitir a visualização de eventuais áreas sem cobertura de RF (áreas de sombra);

9.7.17.2. Visualização do mapa de calor de RF (Heatmap);

9.7.29. Possibilitar a identificação de paredes e divisórias com respectivos níveis de atenuação por tipo (alvenaria, vidro, drywall e divisória);

Sugestão de Alteração: Sem alteração de texto, alteração de posição

Justificativa: A ferramenta da Huawei de planejamento da rede sem fio com visualização da planta baixa dos andares é um software independente e integrável à solução de gerenciamento, encaixando-se na condição descrita pelo subitem "9.7.17.5. Caso esta funcionalidade não esteja disponível no sistema de gerência, deve ser fornecido software, do mesmo fabricante, para atender este item.". Sendo assim, solicitamos que os itens listados acima sejam subitens do item 9.7.17''. Deve possuir informação visual e gráfica, planta baixa dos andares, para:", sem prejuízos ao funcionamento da solução.

Resposta: A sugestão será desconsiderada, pois não foi solicitada alterações

---

Texto Original:

9.7.20. Possuir capacidade de geração de relatórios dos seguintes tipos:

Sugestão de Alteração: 9.7.20. Possuir capacidade de geração de relatórios ou visualização na interface gráfica das seguintes informações:

Justificativa: Solicitamos a alteração para participação.

Resposta: A sugestão será acatada

Texto Original: 9.7.20.6. Suportar SSH, HTTP/HTTPS, SSL, Telnet;

Sugestão de Alteração: Fazer do item um novo tópico.

Justificativa: No texto original o item mencionado é subitem de 9.7.20. Possuir capacidade de geração de relatórios dos seguintes tipos:". Para coerência do texto, sugerimos que seja removido dos subitens do item 9.7.20.

Resposta: A sugestão será acatada.

Criar novo tópico: Suportar SSH, HTTP/HTTPS, SSL, Telnet;

Texto Original: 9.7.22 Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c ou SNMPv3, incluindo a geração de traps;

Sugestão de Alteração: 9.7.22. Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps, ou NETCONF.

Justificativa: A primeira parte da sugestão tem como objetivo assegurar a implementação do SNMPv3, assim como é solicitado no software de gerenciamento item "9.7.22.". O SNMPv3 fornece todas as funções do SNMPv1 e SNMPv2, e apresenta um mecanismo de segurança que autentica e criptografa pacotes SNMP. Em termos de segurança, o SNMPv3 enfatiza a segurança dos dados e o controle de acesso. O SNMPv3 garante a segurança dos pacotes SNMP das seguintes maneiras:

1. Verificação da integridade dos dados Os dados não podem ser modificados de forma não autorizada. A alteração da sequência de dados é limitada à extensão permitida.

2. Autenticação de origem de dados O SNMPv3 autentica o nó gerenciado do qual a origem é recebida e não o aplicativo que gera o pacote.

3. Confidencialidade dos dados: Quando o NMS ou o agente recebem um pacote, verificam a hora em que o pacote é gerado. Se a diferença entre a hora de criação e a hora do sistema exceder o limite, o pacote será descartado. Desta forma, os pacotes que são modificados por mal-intencionados não são aceitos.

A segunda parte da sugestão é a adição de uma alternativa de protocolo de gerenciamento. A sugestão apenas acrescenta uma alternativa, não altera para os fabricantes que implementam a gerência por meio de SNMP.

O NETCONF, assim como o SNMP, é um protocolo aberto e inclusive mais interoperável que o SNMP.

O Network Configuration Protocol (NETCONF) é um protocolo de gerenciamento de rede que permite que um sistema de gerenciamento de rede (NMS) entregue, modifique e exclua configurações de dispositivos de rede.

As interfaces de programação de aplicativos (APIs) padrão estão disponíveis em dispositivos de rede para que o NMS gerencie os dispositivos usando o NETCONF. Para superar as desvantagens da CLI e do SNMP, o

NETCONF baseado em XML é introduzido, que tem as seguintes vantagens:

1. NETCONF usa uma estrutura de protocolo hierárquico, tornando-o mais adequado para requisitos de big data, automatizados e sob demanda de redes baseadas em nuvem.

2. NETCONF usa codificação XML para definir mensagens e usa o mecanismo RPC para modificar dados de configuração. Isso facilita o gerenciamento de dados de configuração e a interoperabilidade entre dispositivos de diferentes fornecedores.

3. O NETCONF realiza operações em dispositivos baseados no modelo YANG, reduzindo falhas de rede causadas por erros de configuração manual.

4. NETCONF fornece mecanismos de segurança, como autenticação e autorização para garantir a segurança da transmissão de mensagens.

5. O NETCONF fornece um mecanismo de transação para oferecer suporte à classificação, armazenamento e migração de dados, envio baseado em fases, isolamento de configuração, bem como entrega, verificação e reversão de configuração geral, minimizando o impacto nos serviços de rede.

Resposta: A sugestão será acatada parcialmente:

“Deve implementar, em conjunto com o controlador WLAN especificado, padrões abertos de gerência de rede SNMPv2c ou SNMPv3, incluindo a geração de traps e/ ou NETCONF”

Texto Original:

9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance, sendo compatível com os seguintes Hypervisors:

9.8.1.1. VmWare ESXi 5.5 ou superior;

9.8.1.2. Microsoft Hyper-V Server 2012 R2/2016 e Windows Server 2012 R2 com Hyper-V;

9.8.1.3. Amazon EC2;

9.8.1.4. CentOS KVM;

Sugestão de Alteração: 9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance. Deverão ser providos quantos softwares e ou appliance forem necessários para realizar as funções de gerenciamento e controle de todos os pontos de acesso e switches contratados, incluindo sistema operacional e todas licenças

necessárias.

Justificativa: A solução ofertada deve incluir os appliances, softwares, sistema operacional e sistemas de virtualização necessários ao funcionamento da solução, não havendo motivos para limitar o tipo de Hypersor utilizado. Dessa forma, solicitamos a alteração para que todos os recursos para o funcionamento pleno da solução sejam entregues, de acordo com as especificações dos diferentes fabricantes.

Resposta: A especificação será readequada

“9.8.1. Os equipamentos devem incluir solução de autenticação de usuários e dispositivos para controle de acesso à rede baseada em appliance físico ou Virtual Appliance. Deverão ser providos quantos softwares e ou appliance forem necessários para realizar as funções de gerenciamento e controle de todos os pontos de acesso e switches contratados, incluindo sistema operacional e todas licenças necessárias.“

Texto Original: 9.8.3. A solução deve ser disponibilizada em infraestrutura da CONTRATADA, devendo ser

transferida para infraestrutura da CONTRATANTE ao fim do contrato ou quando for solicitado.

Sugestão de Alteração: 9.7.7. A solução deve estar instalada em infraestrutura sob responsabilidade da CONTRATADA podendo ser migrado para infraestrutura da CONTRATANTE no término do contrato ou quando for solicitado.

Justificativa: Sugerimos a alteração para a possibilidade da contratação de ambientes de ISPs para implementação da infraestrutura, com o fornecimento de ambiente especializado para os equipamentos.

Resposta: A sugestão não será acatada

Texto Original: 9.8.5. Possuir plataforma unificada que combina AAA, NAC, BYOD e acesso de convidado incorporando identidade, integridade, informações físicas/ de dispositivo e elementos condicionais em um conjunto de políticas.

Sugestão de Alteração: 9.8.5 Possuir plataforma unificada que combina AAA e controle de acesso de usuários convidados.

Justificativa: Solicitamos a substituição pelo texto simplificado para fácil constatação ao atendimento às funcionalidades requeridas através da documentação dos diversos fabricantes. O texto original contém termos que dependem de interpretação. O texto sugerido é claro sobre a solução que está sendo solicitada, com termos utilizados pelos mais diversos fabricantes.

Resposta: A especificação será readequada:
"9.8.5 Possuir plataforma unificada que combina AAA e controle de acesso de usuários convidados."

Texto Original:

9.8.6. Suporte a seguintes fontes para autenticação:

9.8.6.1. Microsoft Active Directory

9.8.6.2. Kerberos

9.8.6.3. LDAP-compliant directory

9.8.6.4. ODBC-compliant SQL server

9.8.6.5. Token servers

9.8.6.6. Base SQL interna

9.8.6.7. Radius

9.8.6.8. Microsoft Azure Active Directory

9.8.6.9. Google G Suite

9.8.6.10. HTTP

9.8.6.11. Lista estática de endereços MAC autenticação:

Sugestão de Alteração:

9.8.6. Suporte a seguintes fontes para autenticação:

9.8.6.1. Microsoft Active Directory

9.8.6.2. LDAP

9.8.6.3. Base SQL interna

9.8.6.4. Radius

9.8.6.5. Google G Suite

9.8.6.6. HTTP

9.8.6.7. Lista estática de endereços MAC autenticação:

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A especificação será readequada para o item 9.8.6 e seus subitens e serão consideradas as especificações a seguir:

9.8.6. Suporte a seguintes fontes para autenticação:

9.8.6.1. Microsoft Active Directory

9.8.6.2. LDAP

9.8.6.3. Base SQL interna

9.8.6.4. Radius

9.8.6.5. Google G Suite

9.8.6.6. HTTP

9.8.6.7. Lista estática de endereços MAC autenticação

Texto Original: 9.8.8. Registro e autenticação de usuário baseado na Web (como autor-registro, sponsor based e social-login).

9.8.8.1. Multifator de autenticação OnConnect

Sugestão de Alteração: 9.8.8. Registro e autenticação de usuário baseado na Web, por meio de auto-registro ou login através de rede social.

9.8.8.1. Multifator de autenticação

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: Para o item 9.8.8. A especificação será readequada:

"9.8.8. Registro e autenticação de usuário baseado na Web, por meio de auto-registro ou login através de rede social."

Resposta: Para o item 9.8.8.1. A especificação será readequada:
"9.8.8.1. Multifator de autenticação"

Remover item: 9.8.9. Recursos do 360 Security Exchange, incluindo servidores de contexto de endpoint locais e ações de servidor de contexto para o host local e XML.

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A especificação será readequada:

"A solução de autenticação deve permitir integração com ferramentas de segurança de terceiros, tipo antivírus, firewall"

Remover item: 9.8.10. Demais recursos devem ser suportados através de upgrades futuros da solução.

Justificativa: Sugerimos a remoção do item. O item não é claro sobre quais recursos devem ser suportados através de upgrades futuros, abrindo espaço para interpretações e entregas de software sem todas as capacidades solicitadas para o projeto.

Resposta: A sugestão não será acatada.

Texto Original: 9.8.12. Permitir a visualização de todas informações relativas a cada transação/autenticação em uma única tela, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise.

Sugestão de Alteração: 9.8.12. Permitir a visualização de todas informações relativas a cada transação/autenticação, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise.

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A sugestão será acatada.

Texto Original: 9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authentication;

Sugestão de Alteração: 9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ ou HWTACACS e Web Authentication;

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A especificação será readequada.

"9.8.13.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ ou similar e Web Authentication;"

Texto Original: 9.8.17. Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex.

Computador, Smartdevice, impressora, etc), por sistema operacional (ex. Windows, Linux, MacOS, etc.) e versão do sistema (ex. Windows 7,

Windows 2008 Server, etc);

Sugestão de Alteração: 9.8.17. Deve categorizar os dispositivos, por tipo de dispositivo (ex. Computador, Smart device, impressora, etc.) e por sistema operacional;

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A especificação será readequada:

"9.8.17. Deve categorizar os dispositivos, por tipo de dispositivo (ex. Computador, Smart device, impressora, etc.) e por sistema operacional"

Texto Original: 9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting;

Sugestão de Alteração: 9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, SNMP e base de assinaturas;

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A especificação será readequada:

"9.8.18. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, SNMP e base de assinaturas;"

Texto Original: 9.8.21. Deve implementar os serviços de autenticação, profiling e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos.

Sugestão de Alteração: 9.8.21. Deve implementar os serviços de autenticação, profiling e autorização para no mínimo 850.000 (oitocentos e cinquenta mil) usuários/dispositivos e até 700.000 (setecentos mil) usuários/dispositivos online, na implementação completa de todas as escolas previstas;

Justificativa: A solução da Huawei de controle de acesso suporta até 2.000.000 (dois milhões) de usuários, e, em sua configuração máxima, até 700.000 (setecentos mil) usuários online. É importante para o projeto ressaltar a diferença entre usuários totais e usuários online na especificação. Sugerimos o esclarecimento.

Resposta: A sugestão não será acatada.

Texto Original:

9.8.25. Deve suportar no mínimo os seguintes métodos de autenticação:

9.8.25.1. EAP-FAST (EAP-MSCHAPv2, EAP-GTC,EAP-TLS)

9.8.25.2. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAPPEAP-Public, EAP-PWD)

9.8.25.3. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)

9.8.25.4. EAP-TLS

9.8.25.5. PAP, CHAP, MSCHAPv1, MSCHAPv2 and EAP-MD5

9.8.25.6. Windows machine authentication

9.8.25.7. SMB v2/v3

9.8.25.8. WPA3 - MPSK

9.8.25.9. RADSec

9.8.25.10. Online Certificate Status Protocol (OCSP)

9.8.25.11. TACACS+

9.8.25.12. WEB Authentication

Sugestão de Alteração:

9.8.25. Deve suportar no mínimo os seguintes métodos de autenticação:

9.8.25.1. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);

9.8.25.2. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP);

9.8.25.3. WPA3

9.8.25.4. TACACS+ ou HWTACACS

9.8.25.5. WEB Authentication

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A sugestão será acatada. Para o item 9.8.25 e seus subitens a especificação será alterada conforme a seguir:

9.8.25. Deve suportar no mínimo os seguintes métodos de autenticação:

9.8.25.1. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);

9.8.25.2. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP);

9.8.25.3. WPA3

9.8.25.4. TACACS+ ou similar

9.8.25.5. WEB Authentication

Texto Original:

9.8.29. Suporte aos seguintes recursos através de IPv6:

9.8.29.1. Administração via WEB e CLI

9.8.29.2. Servidores de autenticação e autorização com endereçamento IPv6;

9.8.29.3. IPv6 Accounting Proxy;

9.8.29.4. Acesso a servidores com endereçamento IPv6 para contexto de endpoints;

9.8.29.5. Syslog, DNS, NTP;

9.8.29.6. Endereçamento IPv6 para VIP (Virtual IP) de alta disponibilidade;

9.8.29.7. Fontes de Syslog para processamento de evento

Sugestão de Alteração: Substituir o item 9.8.29. e seus subitens por:

9.8.29. Suporte a servidores de autenticação e autorização com endereçamento IPv6;

Justificativa: Solicitamos a alteração para participação no certame.

Resposta: A sugestão será acatada parcialmente:
9.8.29. Suporte a servidores de autenticação e autorização com endereçamento IPv6;

9.8.29.1. Fontes de Syslog para processamento de evento

Remover o item: 9.8.29.8. Validações e conformidades:

9.8.29.8.1. FIPS 140-2

9.8.29.8.2. Common Criteria NDcPP + Servidor de autenticação

Justificativa: Solicitamos a remoção para participação no certame.

Resposta: A sugestão será acatada.

Texto Original: 9.8.31. A solução deve permitir a configuração centralizada de políticas em ambientes distribuídos, no qual as políticas serão configuradas em um único elemento para serem distribuídas aos demais que pertençam à mesma "zona"

Sugestão de Alteração: 9.8.31. A solução deve permitir a configuração centralizada de políticas em ambientes distribuídos, no qual as políticas serão configuradas em um único elemento para serem distribuídas aos demais que pertençam a um mesmo grupo

Justificativa: Solicitamos a remoção para participação no certame.

Resposta: A sugestão não será acatada.

Texto Original: 9.8.33. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML e PDF.

Sugestão de Alteração: 9.8.33. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML ou PDF ou CSV ou EXCEL.

Justificativa: Solicitamos a remoção para participação no certame.

Resposta: A especificação será readequada:

9.8.33. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML ou CSV ou EXCEL e PDF.

Subscrevemos e façamos por concluída a audiência pública.

Sem mais a informar o Estado de Minas Gerais encerra e publica a presente Ata.

Documento assinado eletronicamente por **Adilson Rodrigues da Silva**, **Diretor**, em 07/11/2022, às 11:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Daniel Machado Maia**, **Servidor(a) Público(a)**, em 08/11/2022, às 16:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **55654954** e o código CRC **19F78405**.

Referência: Processo nº 1260.01.0120259/2022-61 SEI nº 55654954