TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS
Avenida Aristeu de Andrade nº 377 - Bairro Farol - CEP 57051-090 - Maceió - AL

Termo de Referência - TIC nº 24 / 2019

Termo de Referência - Soluções de Tecnologia da Informação

QUADRO RESUMO

01. Objeto	Registro de Preço para aquisição de componentes de rede (Networking)

02. Quantidade

LOTE 01 - SOLUÇÃO PARTA REDE CABEADA

ITEM	DESCRIÇÃO DOS PRODUTOS/SERVIÇOS	QTD
ITEM 01	SOLUÇÃO DE ANÁLISE DE PERFIL E CONTROLE DE ACESSO PARA REDE CABEADA	01
ITEM 02	LICENCIAMENTO ADICIONAL PARA SISTEMA DE GERENCIAMENTO HPE IMC	03
ITEM 03	LICENCIAMENTO ADICIONAL DO MÓDULO DE ANÁLISE DE TRAFEGO DO SISTEMA DE GERENCIAMENTO HPE IMC	02
ITEM 04	LICENCIAMENTO ADICIONAL DA SOLUÇÃO DE ANÁLISE DE PERFIL E CONTROLE DE ACESSO	02
ITEM 05	SWITCH DE DISTRIBUIÇÃO COM 16 PORTAS SFP+ E SUPORTE A MÓDULOS DE EXPANSÃO	06
ITEM 06	MÓDULO COM 4 PORTAS SFP+ PARA SWITCH DE DISTRIBUIÇÃO	16
ITEM 07	MÓDULO DE STACKING COM 4 PORTAS PARA SWITCH DE DISTRIBUIÇÃO	06
ITEM 08	SWITCH DE ACESSO L3 COM 48 PORTAS GIGABIT E 4SFP+	50
ITEM 09	SWITCH DE ACESSO L3 COM 24 PORTAS GIGABIT E 4SFP+	40
ITEM 10	SWITCH DE ACESSO L2 COM 24 PORTAS GIGABIT E 4SFP	50
ITEM 11	SWITCH DE ACESSO L2 COM 48 PORTAS GIGABIT E 4SFP	40
ITEM 12	GBIC 10GB PARA ATÉ 300M	50
ITEM 13	CABO DAC 10 GBPS DE 1M	30

ITEM 14	CABO DAC 10 GBPS DE 3M	30
ITEM 15	GBIC 1GB PARA ATÉ 500M	10
ITEM 16	SERVIÇOS DE IMPLANTAÇÃO E TRANSFERÊNCIA DE TECNOLOGIA PARA SWITCHS DE REDE	05
ITEM 17	SERVIÇOS DE IMPLANTAÇÃO E TRANSFERÊNCIA DE TECNOLOGIA DO MÓDULO DE CONTROLE DE ACESSO	01
ITEM 18	TREINAMENTO BÁSICO DE ADMINISTRAÇÃO DE SWITCHES	04
ITEM 19	TREINAMENTO BÁSICO DA SOLUÇÃO DE CONTROLE DE ACESSO	04

LOTE 02 - SOLUÇÃO DE REDE WIRELESS

ITEM	DESCRIÇÃO DOS PRODUTOS/SERVIÇOS	QTD
ITEM 01	SOLUÇÃO DE ANÁLISE DE PERFIL E CONTROLE DE ACESSO PARA REDE WIRELESS	01
ITEM 02	SOLUÇÃO DE GERENCIAMENTO DE REDE WIRELESS	01
ITEM 03	LICENÇAS ADICIONAIS PARA SOLUÇÃO DE GERENCIAMENTO DE REDE WIRELESS	200
ITEM 04	LICENCIAMENTO ADICIONAL DA SOLUÇÃO DE ANÁLISE DE PERFIL E CONTROLE DE ACESSO	02
ITEM 05	CONTROLADORA WLAN	04
ITEM 06	LICENÇAS ADICIONAIS PARA CONTROLADORA WLAN	200
ITEM 07	PONTO DE ACESSO INTERNO TIPO 01	100
ITEM 08	PONTO DE ACESSO INTERNO TIPO 02	100
ITEM 09	INJETOR POE PARA PONTOS DE ACESSO TIPO 1	100
ITEM 10	INJETOR POE PARA PONTOS DE ACESSO TIPO 2	100
ITEM 11	SERVIÇOS DE IMPLANTAÇÃO E TRANSFERÊNCIA DE TECNOLOGIA PARA SOLUÇÃO DE GERENCIAMENTO	01

	ITEM 12	SERVIÇOS DE IMPLANTAÇÃO E TRANSFERÊNCIA DE TECNOLOGIA DO MÓDULO DE CONTROLE DE ACESSO	01
	ITEM 13	SERVIÇOS DE IMPLANTAÇÃO E TRANSFERÊNCIA DE TECNOLOGIA PARA PONTOS DE ACESSO	05
	ITEM 14	TREINAMENTO BÁSICO DE ADMINISTRAÇÃO DE ARQUITETURA WLAN	04
	ITEM 15	TREINAMENTO BÁSICO DA SOLUÇÃO DE GERENCIAMENTO	04
	ITEM 16	TREINAMENTO BÁSICO DA SOLUÇÃO DE CONTROLE DE ACESSO	04

03. Resumo da Especificação do Objeto	Por se tratar de quantidade elevata de itens partencente a lotes específicos, o detalhamento das e consntante no DETALHAMENTO DO OBJETO (Art. 18, § 3º, III).
04. Valor Estimado	Os custos totais projetados, por certo, serão objeto de levantamento por parte da Seção de Comp porterior.
05. Justificativa	• A dependência tecnológica para o adequado funcionamento de qualquer instituição é na prática, total; • A malha de comunicação de rede interna é primordial para acesso aos sistemas e serviço informatizados e desta n • Grande parte dos equipamentos de rede do Tribunal está defasado tecnologicamente, fora de garantia ou na iminê mesma; • Permitir a qualificação da equipe da CONIF para o gerenciamento das soluções a serem adquiridas; • Maiores detalhes disponíveis no Item 2 do Documento de Oficialização da Demanda.
06. Prazo de Entrega	O prazo máximo para o fornecimento das licenças é de 90 (noventa) dias corridos após o recebimento da ordem de forne empenho ou documento equivalente. Não podendo ultrapassar, conforme o caso, o dia 15 de dezembro ou dia útil subsec cada exercício individualmente, em decorrência dos efeitos da Emenda Constitucional nº 95/2016
07. Adjudicação	Por Lote. Justificativa: Plena exigência de total compatibilidade e interoperabilidade entre em componentes do respectivo lote, cor à solução de gerenciamento em uso no TRE/AL.
08. Classificação Orçamentária	(A cargo da COFIN).
09. Local de Entrega	Almoxarifado do Tribunal Regional Eleitoral de Alagoas Av. Menino Marcelo, 7200D, Serraria Maceió – AL CEP 57046-005 Tel.: (82) 3328-1947 Horário: De segunda-feira a quinta-feira das 13 às 19h e sexta-feira das 7h30min Às 13h30min.
10. Unidade Fiscalizadora	SEGI/CIE/STI
11. Unidade Gestora	SAD
12. Sanções Administrativas	Vide Item 3.2 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a) Subitem Penalidades (Art. 18, § 3º, III, a, 11)
13. Prazo de Pagamento	Vide Item 3.2 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a) Subitem Forma de Pagamento (Art. 18, § 3º, III, a, 7)
14. Estratégia de Recebimento	Vide Item 3.2 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a) Subitem Recebimento do Objeto:
15. Modalidade e Tipo de Licitação	Vide 2.11 Modalidade, Tipo de Licitação, Critérios de Habilitação e Atendimento aos Requisitos (Art. 18, § 3º, II, j, IV e V)

1. OBJETO (Art. 18, §3º,I):

Registro de Preço para aquisição de componentes de rede sem fio e cabeada.

1.1 Definição (Art. 18, §3º, I)

Registro de Preço para aquisição de computadores para substituir equipamentos fora de garantia e/ou obsoletos.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO (Art. 18, § 3º, II)

2.1 Motivação (Art. 18, § 3º, II, a)

Os equipamentos tem por finalidade a substituição, por atualização tecnológica, de equipamentos, ora em uso, com aproximadamente 04 (quatro) anos e já não mais cobertos por garantia. Estes aspectos, a um só tempo, a se falar em TI, evidenciam a necessidade de atualização e de demanda de salvaguarda, esculpida em garantia, da efetividade e continuidade do mister da Secretaria.

A estratégia de Registro de Preços está amparada no Decreto nº 7.892/2013, art 3º, incisos:

I - vez que os equipamentos podem ser objeto de diversas aquisições/fornecimentos até que se supra progressivamente toda a demanda de substituição progressiva;

II - as entregas deve ser progressivas de forma que as equipes da STI, em número limitado, possam implantar os equipamentos sem que os mesmo precisem ser estocados por longos períodos apenas exaurindo seus prazos de garantia.

2.2 Objetivos (Art. 18, § 3º, II, b)

A contratação visa, além de promover ações no sentido de elaborar novo instrumento que mantenha um meio para disponibilizar os computadores demandados e:

Garantir a infraestrutura física apropriadas às atividades administrativas e judiciais.

Prover infraestrutura de TIC apropriada às atividades judiciais e administrativas.

2.3 Benefícios (Art. 18, § 3º, II, c)

- Reposição de equipamentos defasados e manutenção da capacidade produtiva atualizada.

2.4 Alinhamento Estratégico (Art. 18, § 3º, II, d)

O alinhamento com o PEI é identificado na visão do recursos de infraestrutura e tecnologia em seus dois aspectos apontados:

- Garantir a infraestrutura física apropriadas às atividades administrativas e judiciais.

Alinhamento com os Objetivos Estratégicos da Estratégia Nacional de TIC do Poder Judiciário nos seguintes aspectos:

- Prover infraestrutura de TIC apropriada às atividades judiciais e administrativas.

Alinhamento com os Objetivos Estratégicos de TIC da Justiça Eleitoral de Alagoas – 2017/2022 nos seguintes aspectos:

- Viabilizar serviços e soluções de TIC.

2.5 Referência aos Estudos Preliminares (Art. 18, § 3º, II, e)

Este Termo de Referência foi elaborado considerando o Documento de Oficialização de Demanda (DOD) encaminhado pela Secretaria de Tecnologia da Informação (STI) e os Estudos Preliminares constantes do Processo SEI nº 0008478-63.2018.6.02.8000.

2.6 Relação entre a Demanda Prevista e a Contratada (Art. 18, §3º, II, f)

É pretendida a renovação do parque de equipamentos componentes da infraestrutura de TIC.

2.7 Análise de Mercado de TIC (Art. 18, § 3º, II, g)

Verifica-se que os bens e serviços pretendidos poderão ser fornecidos por diferentes empresas no mercado de TIC.

Considerando o Item 7 dos Estudos Preliminares, não se vislumbrou alternativa que não o presente Registro de Preços.

2.8 Natureza do Objeto (Art. 18, § 3º, II, h)

Os bens e serviços a serem contratados possuem características comuns e usuais encontradas atualmente no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos neste Termo de Referência.

O objeto desta contratação tem como escopo a obtenção de produto específico em período determinado, portanto não se caracteriza como serviço de natureza continuada.

2.9 Parcelamento e Adjudicação do Objeto (Art. 18, § 3º, II, i)

Não haverá parcelamento, cada ordem de fornecimento derivado do Registro de Preços deverá ser realizada de maneira integral.

Adjudicação será por lote.

2.10 Vigência

Será, na forma dos normativos vigentes, o tempo máximo do Registro de Preços.

A vigência da ata será de 12 (doze) meses, contados a partir de sua assinatura.

A utilização do sistema de Registro de Preços visa, primordialmente, a redução de número de licitações para o mesmo objeto, porquanto se concentra em um único procedimento a possibilidade de realizar diversas aquisições recorrentes e necessárias, via ordens de fornecimento, durante o lapso temporal de sua vigência, em face de os preços permanecerem à disposição da Administração.

2.11 Modalidade, Tipo de Licitação, Critérios de Habilitação e Atendimento aos Requisitos (Art. 18, § 3º, II, j, IV e V)

A aquisição pretendida deverá ser realizada por meio de licitação do tipo Pregão Eletrônico, como é de praxe neste Regional, salvo entendimento superior contrário.

A sugestão da equipe de planejamento, por se tratar de fornecimento de equipamento, é pela contratação por licitação via pregão. Por conta de possibilidade de contingenciamento orçamentário indicamos a modalidade de registro de preços.

O DECRETO Nº 7.174, DE 12 DE MAIO DE 2010 que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União deve ser aplicado nesta aquisição por se tratar de bem de informática.

A ressalva que a equipe aponta é em relação ao artigo 3º, item II que versa sobre a necessidade de exigências, na fase de habilitação, de certificações emitidas por instituições públicas ou privadas credenciadas pelo Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (Inmetro), que atestem, conforme regulamentação específica, a adequação à segurança para o usuário e instalações, compatibilidade eletromagnética e consumo de energia.

Tal exigência inviabiliza e restringe a competição deste certame, vez que a certificação para este tipo de produto, segundo o próprio INMETRO, é voluntária, conforme Portaria Inmetro n.º 170 de 10/04/2012.

(fonte:http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC001808.pdf).

pretendida deverá ser realizada por meio de licitação do tipo Pregão Eletrônico, como é de praxe neste Regional, salvo entendimento superior contrário.

A sugestão da equipe de planejamento, por se tratar de fornecimento de equipamento, é pela contratação por licitação via pregão. Por conta de possibilidade de contingenciamento orçamentário indicamos a modalidade de registro de preços.

O DECRETO Nº 7.174, DE 12 DE MAIO DE 2010 que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União deve ser aplicado nesta aquisição por se tratar de bem de informática.

A ressalva que a equipe aponta é em relação ao artigo 3º, item II que versa sobre a necessidade de exigências, na fase de habilitação, de certificações emitidas por instituições públicas ou privadas credenciadas pelo Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (Inmetro), que atestem, conforme regulamentação específica, a adequação à segurança para o usuário e instalações, compatibilidade eletromagnética e consumo de energia.

Tal exigência inviabiliza e restringe a competição deste certame, vez que a certificação para este tipo de produto, segundo o próprio INMETRO, é voluntária, conforme Portaria Inmetro n.º 170 de 10/04/2012.

(fonte:http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC001808.pdf).

2.12 Adequação do Ambiente (Art. 18, § 3º, II, k)

Para utilização do objeto pretendido é necessário dispor de infraestrutura física para sua instalação, situação essa já existente no âmbito do TRE/AL, salvo o surgimento de demanda muito particular e além da previsibilidade.

2.13 Conformidade Técnica e Legal (Art. 18, § 3º, II, l)

2.14 Obrigações do Contratante (Art. 18, § 3º, II, m)

1. Efetuar o pagamento à Contratada, após o recebimento definitivo;
2. Acompanhar e fiscalizar a execução do objeto da Ata de Registro de Preços e do(s) contrato(s) dela decorrentes, por meio de servidor(es) designado(s), de modo a garantir o fiel cumprimento do mesmo e da proposta;
3. Manter arquivo, junto ao processo administrativo ao qual está vinculado o presente termo, toda a documentação referente ao mesmo;
4. Proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais; e
5. Aplicar as sanções conforme previsto no contrato, assegurando à Contratada o contraditório e ampla defesa.

2.15 Obrigações da Contratada (Art. 18, § 3º, II, m)

As obrigações abaixo são aplicáveis ao objeto a ser contratado.

1. Fornecer o(s) equipamento(s) conforme especificações, quantidades, prazos e demais condições estabelecidas no Edital, na Ata de Registro de Preços, na Ordem de Fornecimento, na Proposta e no Contrato;
2. Fornecer a documentação necessária à instalação e à operação dos produtos (manuais, termos de garantia, etc.), completa, atualizada e em português do Brasil, caso exista, ou em inglês;
3. Disponibilizar Central de Atendimento para a abertura e fechamento de chamados técnicos, conforme períodos, horários e condições estabelecidas no Edital e em seus Anexos;
4. Comunicar formal e imediatamente ao Gestor ou Responsável Técnico da Administração sobre mudanças nos dados para contato com a Central de Atendimento;
5. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo representante da Administração, referentes a qualquer problema detectado ou ao andamento de atividades da garantia;
6. Responder por quaisquer prejuízos que seus profissionais causarem ao patrimônio da Administração ou a terceiros, por ocasião da execução do objeto, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente;
7. Responsabilizar-se integralmente pelo fornecimento dos equipamentos e pela execução dos serviços de garantia técnica, primando pela qualidade, desempenho, eficiência e produtividade na execução dos trabalhos, dentro dos prazos estipulados e cujo descumprimento será considerado infração passível de aplicação das penalidades previstas neste Termo de Referência;
8. Comunicar ao Gestor ou Responsável Técnico, formal e imediatamente, todas as ocorrências anormais e/ou que possam comprometer a execução do objeto;
9. Manter sigilo sobre todo e qualquer assunto de interesse da Administração ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa;
10. Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do TRE/AL;
11. Responsabilizar-se pela conservação dos ambientes onde desempenhe as atividades necessárias para prestar a garantia on-site.
12. Prestar as informações e os esclarecimentos que venham a ser solicitados pela Administração, referentes a qualquer problema detectado ou ao andamento de atividades da garantia técnica
13. **No caso de fornecimento/entrega, em final de exercício e posterior ao dia 15 de dezembro ou dia útil imediatamente subsquente, fica obrigado a aceitar, o cancelamento da ordem de fornecimento por parte da Administração, em decorrência dos efeitos da Emenda Constitucional nº 95/2016, sem a reversão de qualquer ônus à Administração.**

DETALHAMENTO DO OBJETO (Art. 18, § 3º, III)

3.1 Descrição do Objeto

CONDIÇÕES GERAIS

1. Todos os itens ofertados por lote, deverão ser do mesmo fabricante para garantir total compatibilidade entre todos os componentes, sem a utilização de ferramentas de terceiros ou modo de interoperabilidade na solução;
2. Para o Lote 01: Todos os itens de software ofertados deverão possuir integração total com o HPE Intelligent Managment Center (IMC) já existente na infraestrutura da contratante, através de interface única de gerenciamento e/ou autenticação centralizada;
3. Para o Lote 01: Os equipamentos fornecidos deverão ser gerenciados pelo HPE IMC já existente na infraestrutura da contratante, com presença na matriz de compatibilidade comprovada através de documentação oficial do fabricante;
4. Os equipamentos devem ser novos e estar em produção. Não serão aceitos equipamentos descontinuados, recondicionados ou usados;
5. Os equipamentos devem ser entregues acondicionados adequadamente em suas embalagens originais;
6. A(s) solução(ões) de gerenciamento/controle ofertada(s), deverá(ão) ser baseada(s) em plataforma “On Premise”, ou seja, deverá ser executada localmente, não sendo aceitas soluções híbridas ou em Cloud;
7. Cada lote deverá ser fornecido por uma única empresa, visando a garantia integral de compatibilidade dos componentes ofertados;
8. As configurações e especificações aqui apresentadas são mínimas, sendo aceitos equipamentos/softwares com características superiores, desde que compatíveis com as exigidas;
9. Prazo de entrega para equipamentos: 60 (sessenta) dias contados a partir da emissão da ordem de fornecimento ou documento equivalente;
10. Prazo de entrega para softwares: 30 (trinta) dias contados a partir da emissão da ordem de fornecimento ou documento equivalente;
11. Os serviços de instalação, integração, garantia e suporte dos equipamentos e softwares, deverão ser realizados diretamente pelo fabricante de acordo com as exigências contidas no descritivo dos mesmos, estando essas aderentes aos respectivos níveis de serviço necessários a cada um deles.

LOTE 01 – SOLUÇÃO DE REDE CABEADA

ITEM 01 – SOLUÇÃO DE ANÁLISE DE PERFIL E CONTROLE DE ACESSO

LICENCIAMENTO

1. Licenciamento da **SOLUÇÃO DE ANÁLISE DE PERFIL E CONTROLE DE ACESSO**, contemplando o quantitativo mínimo de 1.000 (um mil) dispositivos, usuários corporativos ou visitantes simultâneos, independente do perfil de autenticação, seja por dispositivo ou usuário;
2. Caso a solução ofertada necessite de licenciamento específico para credenciamento dos dispositivos, usuários (corporativos ou visitantes), deverá ser fornecido o quantitativo solicitado para ambos, de forma que a solução realize a análise de perfil e o controle de acesso dos 1.000 (um mil) dispositivos ou usuários (corporativos ou visitantes) simultâneos.

MÓDULO DE ANÁLISE DE PERFIL DE DISPOSITIVO

Características Gerais Modulo de Análise de Perfil de Dispositivo

3. Deve implementar funcionalidade de classificação automática criando perfis de dispositivos, de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;
4. Deve categorizar os dispositivos em pelo menos 3 níveis:
    a. Por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.);
    b. Por sistema operacional (ex. Windows, Linux, MacOS, etc.);
    c. Versão do sistema operacional (ex. Windows 7, Windows 2008 Server, etc.);
5. Deve ser capaz de gerar gráficos das categorias, separando os dispositivos conforme suas características;
6. Deve suportar a coleta de informações, para classificação, usando no mínimo:
    a. DHCP;
    b. HTTP User-Agent;
    c. MAC OUI;
    d. ActiveSync plugin;
    e. SNMP;
    f. Subnet Scanner;
    g. IF-MAP;

h. Cisco Device Sensor;

i. MDM;

j. TCP Fingerprinting.

7. Deve possuir dicionário de categorias de dispositivos pré-configurado e mecanismo de atualização do mesmo;

8. Deve suportar a integração com, no mínimo, as seguintes soluções de MDM de mercado AirWatch, MobileIron, BES, JAMF, SOTI, XenMobile, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;

9. Deve permitir priorização na ordem de criação dos perfis com no mínimo as seguintes características:

a. Agente proprietário;

b. HTTP User-Agent;

c. SNMP;

d. DHCP;

e. MAC OUI.

10. A solução de análise de perfil de usuários deverá permitir consultas a sua base, pela solução de controle de acesso para validação de dispositivos com base no seu perfil.

MÓDULO DE CONTROLE DE ACESSO DE DISPOSITIVOS E USUÁRIOS

Características Gerais

11. A Solução deverá dar suporte a no mínimo as seguintes bases de dados:

a. Microsoft Active Directory;

b. Kerberos;

c. Diretórios LDAP;

d. OpenLDAP;

e. PostgreSQL;

f. Oracle 11g;

g. MariaDB;

h. MSSQL;

i. Servidores de Token;

j. Base de dados SQL interna;

k. Lista interna estática de hosts.

12. Deve suportar "Single Sign-on" (SSO) através de SAML v2.0;

13. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

a. Atributos do usuário autenticado;

b. Hora do dia, dia da semana;

c. Tipo de dispositivo utilizado;

d. Localização do usuário;

e. Tipo de autenticação utilizada.

14. Deve permitir a visualização de todas informações relativas a cada transação e autenticação em uma única tela, a solução deverá trazer no mínimo as seguintes informações:

a. Data e Hora;

b. Mac Address do dispositivo;

c. Classificação do dispositivo;

d. Usuário;

e. Equipamento que requisitou a autenticação (origem);

f. Método de autenticação utilizado;

g. Fonte de autenticação utilizada para validação;

h. Perfil de acesso aplicado;

i. Atributos de entrada do protocolo utilizados na requisição (ex. RADIUS);

j. Informações de resposta da solução para o elemento de rede;

k. Alertas em caso de falha;

l. LOGS já filtrados para a requisição em análise.

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

a. a. Lista com últimos Alertas do sistema;

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

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

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

e. Últimas falhas de autenticação;

f. Gráfico com as requisições de avaliação de postura dos dispositivos, divididos em:

- I. Saudáveis (dentro das políticas estabelecidas);

II. Não saudáveis (que estão fora das políticas estabelecidas);

a. a. Lista com as últimas autenticações;

b. Lista com as últimas autenticações com sucesso;

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

16. Deve possuir base de regras e categorias de dispositivos pré-configurada e mecanismo de atualização da mesma;

17. Deve suportar a integração com no mínimo as seguintes soluções de MDM de mercado AirWatch, MobileIron, BES, JAMF, SOTI, XenMobile, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;

18. Deve suportar autenticações via OAuth2, Facebook, Twitter, LinkdIn, Office365 e Google Apps;

19. Deve possuir recursos integrados de AAA: RADIUS, TACACS+ e Kerberos;

20. Deve possuir suporte aos seguintes recursos:

a. RADIUS;

b. RADIUS CoA;

c. TACACS+;

d. Web authentication;

e. SAML v2.0;

f. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);

g. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public);

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

i. EAP-TLS;

j. PAP, CHAP, MSCHAPv1, MSCHAPv2 e EAP-MD5;

k. Windows machine authentication;

l. MAC address authentication (dispositivos sem suporte a 802.1X);

21. Deve suportar verificação de vulnerabilidade através de varredura de portas;

22. Deve suportar à aplicação de políticas em ambiente com múltiplos fornecedores de Wireless, cabeado e VPN;

23. Deve possuir CA integrada, para geração de certificados para os dispositivos que forem se autenticar na rede;

24. Deve suportar à integração com plataforma de terceiros usando HTTP/RESTful API;

25. Deve permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários;

26. Deve possuir suporte a administração através de IPv6;

27. Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilização de usuários visitantes através de portal web seguro;

28. Deve implementar a criação de grupos de autorizadores com privilégios distintos de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;

29. Deve permitir realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;

30. Deve implementar as funcionalidades de geração de lotes de credenciais aleatórias, temporárias, pré-autorizadas;

31. Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;

32. Deve permitir a configuração do tempo de validade das credenciais, baseando-se na criação da conta ou no primeiro login da conta;

33. Deve permitir que o visitante crie sua própria credencial temporária (autosserviço) através de portal web, com ou sem a necessidade de um autorizador;

34. Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante em caso de autosserviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;

35. Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha;

36. Deve exigir que o usuário visitante aceite o "Termo de uso da rede" a cada login ou apenas no primeiro login;

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

GARANTIA E SUPORTE

38. Garantia e suporte do fabricante para a solução de software ofertada pelo período mínimo de 36 (sessenta) meses, incluindo a evolução para novas versões devendo o atendimento ser na modalidade 24x7 (vinte quatro horas por dia, sete dias da semana), com tempo de resposta máximo em 4 (quatro) horas;

39. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante ("part number"), incorporada à solução;

40. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como "chat" e "e-mail" em seu site da internet com disponibilidade ainda de área para cadastro da solução de software ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções ("hotfix") da solução;

41. A empresa fabricante da solução de software deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

42. A comprovação da modalidade da garantia deverá ocorrer através de documentação do fabricante de domínio público, não sendo aceita documentação emitida pelo fornecedor ou centro de distribuição para fins de comprovação que por ventura conflitem com catálogos, manuais, folders oficiais impressos ou da internet (devendo constar o endereço URL para folders da web). Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos softwares, indicando o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante deverá ser anexada a mesma a procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.

ITEM 02 – LICENCIAMENTO ADICIONAL PARA SISTEMA DE GERENCIAMENTO HPE IMC

Características técnicas mínimas

1. Licenciamento para expansão do **SISTEMA DE GERENCIAMENTO HPE IMC** existente na infraestrutura da contratante, contemplando o quantitativo adicional mínimo de 50 (cinquenta) dispositivos simultâneos;

GARANTIA E SUPORTE

1. Garantia e suporte do fabricante para a solução de software ofertada pelo período mínimo de 36 (sessenta) meses, incluindo a evolução para novas versões devendo o atendimento ser na modalidade 24x7 (vinte quatro horas por dia, sete dias da semana), com tempo de resposta máximo em 4 (quatro) horas.

2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante ("part number"), incorporada à solução.

3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como "chat" e "e-mail" em seu site da internet com disponibilidade ainda de área para cadastro da solução de software ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções ("hotfix") da solução;

4. A empresa fabricante da solução de software deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

5. A comprovação da modalidade da garantia deverá ocorrer através de documentação do fabricante de domínio público, não sendo aceita documentação emitida pelo fornecedor ou centro de distribuição para fins de comprovação que por ventura conflitem com catálogos, manuais, folders oficiais impressos ou da internet (devendo constar o endereço URL para folders da web). Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos softwares, indicando o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante deverá ser anexada a mesma a procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.

ITEM 03 – LICENCIAMENTO ADICIONAL DO MÓDULO DE ANÁLISE DE TRAFEGO DO SISTEMA DE GERENCIAMENTO HPE IMC

Características técnicas mínimas

1. Licenciamento para expansão do **MÓDULO DE ANÁLISE DE TRAFEGO DO SISTEMA DE GERENCIAMENTO HPE IMC** existente na infraestrutura da contratante, contemplando o quantitativo adicional mínimo de 5 (cinco) dispositivos simultâneos;

GARANTIA E SUPORTE

1. Garantia e suporte do fabricante para a solução de software ofertada pelo período mínimo de 36 (sessenta) meses, incluindo a evolução para novas versões devendo o atendimento ser na modalidade 24x7 (vinte quatro horas por dia, sete dias da semana), com tempo de resposta máximo em 4 (quatro) horas.

2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante ("part number"), incorporada à solução.

3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de software ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;

4. A empresa fabricante da solução de software deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

5. A comprovação da modalidade da garantia deverá ocorrer através de documentação do fabricante de domínio público, não sendo aceita documentação emitida pelo fornecedor ou centro de distribuição para fins de comprovação que por ventura conflitem com catálogos, manuais, folders oficiais impressos ou da internet (devendo constar o endereço URL para folders da web). Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos softwares, indicando o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante deverá ser anexada a mesma a procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.

ITEM 04 – LICENCIAMENTO ADICIONAL DA SOLUÇÃO DE ANÁLISE DE PERFIL E CONTROLE DE ACESSO

Características técnicas mínimas

2. Licenciamento para expansão da **SOLUÇÃO DE ANALISE DE PERFIL E CONTROLE DE ACESSO**, contemplando o quantitativo mínimo adicional de 500 (quinhentos) dispositivos, usuários corporativos ou visitantes simultâneos, independente do perfil de autenticação, seja por dispositivo ou usuário;

GARANTIA E SUPORTE

1. Garantia e suporte do fabricante para a solução de software ofertada pelo período mínimo de 36 (sessenta) meses, incluindo a evolução para novas versões devendo o atendimento ser na modalidade 24x7 (vinte quatro horas por dia, sete dias da semana), com tempo de resposta máximo em 4 (quatro) horas.

2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.

3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de software ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;

4. A empresa fabricante da solução de software deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

5. A comprovação da modalidade da garantia deverá ocorrer através de documentação do fabricante de domínio público, não sendo aceita documentação emitida pelo fornecedor ou centro de distribuição para fins de comprovação que por ventura conflitem com catálogos, manuais, folders oficiais impressos ou da internet (devendo constar o endereço URL para folders da web). Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos softwares, indicando o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante deverá ser anexada a mesma a procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.

ITEM 05 – SWITCH DE DISTRIBUIÇÃO COM 16 PORTAS SFP+ E SUPORTE A MÓDULOS DE EXPANSÃO

Características técnicas mínimas

1. Deve possuir no mínimo 16 portas 10 Gigabit Ethernet, 1000/10000 SFP+ fixas ao equipamento

2. Deve suportar, através de módulos, o mínimo de 8 portas adicionais de 10 Gigabit Ethernet SFP+ ou 2 portas de 40 Gigabit Ethernet QSFP+;

3. Deve suportar transceivers de 10GbE SFP+ e de 40GbE QSFP+ através da adição ou substituição de módulos.

4. Deve possuir, no mínimo, 2 módulos de expansão podendo ser utilizados para uplinks ou dados de usuários;

5. Deve possuir, no mínimo, 2 módulos de fonte internas ao equipamento operando em modo redundante;

6. Deve possuir porta dedicada de gerenciamento;

7. Deve possuir 1 interface RJ-45 ou serial para acesso console local;

8. Deve possuir latência de, no máximo, 2,8 µs a 1Gbps;

9. Deve possuir memória SDRAM de no mínimo 2 Gbytes;

10. Deve possuir buffer de pacotes de no mínimo 13.5 Mbytes;

11. Deve possuir capacidade de encaminhamento de no mínimo 285 Mpps;

12. Deve possuir capacidade de comutação de no mínimo 480 Gbps;

13. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;

14. Deve possuir fonte de alimentação interna 110/220VAC;

Disponibilidade

15. Deve possuir capacidade de, no mínimo, 10 (dez) equipamentos membros da mesma pilha;

16. Deve possuir fonte de alimentação interna redundante com características idênticas a fonte principal;

17. Deve suportar empilhamento com banda agregada mínima de 320 Gbps sem uso de portas de dados de usuário para este fim.

Switching

18. Deve implementar VLANs baseadas em MAC;
19. Deve suportar no mínimo 4094 VLAN IDs;
20. Deve implementar registro dinâmico de VLAN com MVRP;
21. Deve suportar protocolo OpenFlow 1.3;
22. Deve implementar Jumbo frames nas interfaces Gigabit Ethernet e 10-Gigabit Ethernet
23. Deve implementar Jumbo frames com tamanho de até 9000 bytes;
24. Deve implementar Ethernet link aggregation;
25. Deve implementar IEEE 802.1ad QinQ;
26. Deve suportar agregação de link através de LACP com no mínimo 144 grupos distribuídos através da pilha, com cada grupo permitindo até 8 portas;
27. Deve implementar IEEE 802.3x Flow Control;
28. Deve implementar STP BPDU Protection (BPDU Guard);
29. Deve implementar IEEE 802.1w Rapid Reconfiguration of Spanning Tree;
30. Deve implementar MSTP IEEE 802.1s com pelo menos 64 instâncias;
31. Deve implementar UDLD ou DLDP.

Roteamento

32. Deve implementar roteamento estático IPv4 e IPv6;
33. Deve implementar RIP, RIPv2 e RIPng;
34. Deve possuir no mínimo 512 interfaces de roteamento IP (VLAN Interface)
35. O equipamento ofertado deve implementar roteamento baseado em política (PBR) para IPv4 e IPv6;
36. O equipamento ofertado deve possuir tabela de roteamento com no mínimo 10 mil entradas IPv4 e 5 mil entradas IPv6;
37. Deve suportar no mínimo 256 rotas estáticas;
38. O equipamento ofertado deve permitir autenticação em servidores RADIUS e TACACS+;
39. Deve suportar dual stack IPv4/IPv6;
40. Deve implementar Bidirectional Forwarding Detection (BFD), suportando redução do tempo de convergência para OSPF e VRRP;
41. Deve implementar OSPF v2 e OSPF v3;
42. Deve implementar BGP.

QoS

43. Deve implementar 8 filas em cada porta;
44. Deve implementar traffic shapping;
45. Deve implementar classificação de tráfego utilizando informações de camada 2, 3 e 4;
46. Deve implementar priorização do trafego em camada 4, baseado em número de portas TCP/UDP.

Segurança

47. Deve implementar autenticação 802.1x de múltiplos usuários por porta, simultaneamente.
48. Deve implementar segurança orientada por identidade e controle de acesso por usuário através de ACLs que permitam ou negue o acesso do usuário aos recursos de rede específicos, com base na identidade do usuário.
49. Atribuição VLAN automática, automaticamente atribui os usuários para a VLAN apropriada, com base em suas identidades.
50. Deve implementar accounting RADIUS;
51. Deve implementar TACACS+;
52. Deve implementar proteção contra ataques de ARP;
53. Deve implementar proteção contra IP spoofing (IP source guard);
54. Deve implementar SNMP v1, v2 e v3;
55. Deve implementar detecção de ataques maliciosos e enviar um aviso quando uma anomalia potencial, causada pelos ataques mal-intencionado, for detectado.
56. Deve suportar o isolamento de portas e VLANs, de forma que uma porta ou VLAN isolada não possa enviar tráfego para outra porta isolada do mesmo switch;
57. Deve implementar segurança do gerenciamento do switch em métodos de acesso CLI, GUI ou MIB, através de SSHv2, SSL e SNMPv3
58. Deve implementar autenticação baseado em porta ou endereço MAC;

59. Deve implementar autenticação utilizando navegadores web, possibilitando que clientes que não possuem cliente 802.1x possam autenticar;
60. Deve suportar port-security.

Gerenciamento

61. Deve permitir instalação simplificada “Zero-touch provisioning” através de processo baseado em DHCP com a solução de software de gerenciamento;
62. O equipamento ofertado deve permitir múltiplos arquivos de configuração;
63. Deve suportar espelhamento remoto;
64. Deve implementar Secure File Transfer Protocol;
65. Deve implementar LLDP;
66. Deve implementar LLDP-MEd;
67. Deve implementar SNTP v4;
68. O equipamento ofertado deve Implementar Sflow ou Netflow;
69. Deve implementar RFC 1213 MIB II;
70. Deve implementar RFC 2096 IP Forwarding Table MIB;
71. Deve implementar RFC 2571 SNMP Framework MIB;
72. Deve implementar RFC 2572 SNMP-MPD MIB;
73. Deve implementar RFC 2573 SNMP-Notification MIB;
74. Deve implementar RFC 2574 SNMP USM MIB;
75. Deve implementar RFC 2737 Entity MIB (Version 2);
76. Deve implementar RFC 3414 SNMP-User based-SM MIB;
77. Deve implementar RFC 3415 SNMP-View based-ACM MIB;
78. Deve implementar RFC 2668 802.3 MAU MIB;
79. Deve implementar RFC 3418 MIB for SNMPv3;
80. Deve ser fornecido com a versão de software mais completa e atual disponível para o equipamento;
81. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
82. O equipamento ofertado deve possuir certificado de homologação na Anatel, de acordo com a resolução n° 242;

Garantia e Suporte

83. O equipamento ofertado deverá possuir garantia do fabricante na modalidade on-site pelo período mínimo de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento. O prazo máximo para atendimento do chamado deve ser de até o próximo dia útil após a sua abertura. Durante o período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis.
84. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.
85. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de hardware ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;
86. A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.
87. Para efeito de comprovação da garantia, suporte, dos níveis de atendimento e solução exigidos para os equipamentos, deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante a esta deverá ser anexada uma procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.
88. Todos os componentes instalados ou integrados dos equipamentos devem ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 06 – MÓDULO COM 4 PORTAS SFP+ PARA SWITCH DE DISTRIBUIÇÃO

Características técnicas mínimas

1. Módulo de expansão para switch de distribuição;
2. Suporte a no mínimo 4 (quatro) portas SFP+;
3. Deve ser compatível com GBICS 100M/1G/10G SFP+;

4. Deve possuir suporte a MACsec;

5. Compatibilidade integral com o item 05.

Garantia e Suporte

6. O equipamento ofertado deverá possuir garantia do fabricante do equipamento na modalidade on-site pelo período mínimo de 12 (doze) meses para reposição de peças, mão de obra e atendimento no local. O período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis;

7. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (part number), incorporado ao equipamento;

8. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada;

ITEM 07 – MÓDULO DE STACKING COM 4 PORTAS PARA SWITCH DE DISTRIBUIÇÃO

Características técnicas mínimas

1. Módulo de expansão para switch de distribuição;

2. Suporte a no mínimo 4 (quatro) portas para stacking;

3. Deve prover no mínimo 320Gbps por módulo;

4. Deve acompanhar 1 (um) cabo de stacking compatível, com 1 (um) metro de comprimento;

5. Compatibilidade integral com o item 05.

Garantia e Suporte

6. O equipamento ofertado deverá possuir garantia do fabricante do equipamento na modalidade on-site pelo período mínimo de 12 (doze) meses para reposição de peças, mão de obra e atendimento no local. O período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis;

7. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (part number), incorporado ao equipamento;

8. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada;

ITEM 08 – SWITCH DE ACESSO L3 COM 48 PORTAS GIGABIT E 4 SFP+

Características gerais

1. Deve possuir 48 portas 10/100/1000;

2. Deve possuir 4 portas 1/10G SFP+;

3. Deve possuir capacidade de encaminhamento de, no mínimo, 110 Mpps;

4. Deve possuir capacidade de comutação de, no mínimo, 176 Gbps;

5. Deve implementar IEEE 802.3az para as portas 10/100/1000;

6. Deve possuir uma interface de console USB;

7. Deve suportar empilhamento de no mínimo 8 switches;

8. Deve suportar agregação de link através de LACP com no mínimo 20 grupos distribuídos através da pilha, com cada grupo permitindo até 8 portas;

9. Deve suportar a agregação de links entre diferentes membros da pilha;

10. Deve possuir no mínimo 32.000 endereços MAC;

11. Deve possuir latência máxima de 4µs, considerando pacotes de 64 bytes;

12. Deve possuir buffers de, no mínimo, 12 MB;

13. Deve implementar funcionalidade que permita a detecção de links unidirecionais;

14. Deve implementar funcionalidade que permita a detecção de falhas de uplink;

15. Deve implementar no mínimo 2000 VLANs simultaneamente;

16. Deve implementar MVRP (Multiple VLAN Registration Protocol);

17. Deve implementar LLDP (IEEE 802.1ab);
18. Deve implementar LLDP-MED;
19. Deve implementar Q-in-Q (IEEE 802.1ad);
20. Deve implementar PVST+, RPVST+ ou protocolo compatível;
21. Deve implementar MSTP (IEEE 802.1s);
22. Deve implementar túneis VxLAN (VTEP).

Funcionalidades de Camada 3

23. Deve possuir tabela de roteamento com no mínimo 2.000 rotas IPv4 e 1.000 rotas IPv6;
24. Deve implementar roteamento estático;
25. Deve implementar RIP v2, com suporte a autenticação MD5 (RIPv2);
26. Deve implementar RIPng;
27. Deve implementar OSPF;
28. Deve implementar OSPFv3;
29. Deve implementar Policy-based Routing;
30. Deve implementar VRRP;
31. Deve implementar VRRPv3;
32. Deve implementar servidor DHCP;
33. Deve implementar DHCP snooping (IPv4 e IPv6);
34. Deve implementar DHCP relay (IPv4 e IPv6);
35. Deve implementar Gateway mDNS, com suporte a Apple Bonjour.

Multicast

36. Deve implementar PIM-SM;
37. Deve implementar PIM-DM;
38. Deve implementar MLD snooping;
39. Deve implementar IGMP v3.

Software Defined Networking

40. Deve implementar OpenFlow 1.3 ou superior;
41. Deve implementar a separação lógica do tráfego sem suporte a OpenFlow do tráfego com suporte a OpenFlow através de instâncias. O tráfego OpenFlow não pode influenciar o tráfego não openflow no equipamento;
42. Deve permitir configurar cada instância como modo ativo (pacotes referentes a fluxos que o switch não conhece são enviados para a controladora) ou modo passivo (pacotes que não se referem a um fluxo na tabela do switch não são enviados para a controladora);
43. Deve implementar 16 instâncias de OpenFlow;
44. As instâncias de OpenFlow devem suportar a associação de múltiplas VLANs;
45. Cada instância OpenFlow configurada no equipamento deve suportar, pelo menos, a configuração de 3 controladores SDN;
46. Deve permitir utilizar intervalo de portas TCP/UDP e flags de TCP como parâmetros nas regras de OpenFlow;
47. Deve suportar no mínimo 16.000 regras openflow;
48. Deve possuir interface REST API;
49. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE;
50. Deve suportar a criação de VLANs e ACLs no equipamento através de REST.

QoS

51. Deve implementar controle de broadcast;
52. Deve implementar rate limiting para pacotes ICMP;
53. Deve implementar rate limiting para tráfego broadcast e multicast;

54. Deve implementar rate limiting baseado em tráfego classificado por uma ACL;
55. Deve suportar espelhamento de portas;
56. Deve suportar espelhamento de tráfego para um switch remoto.

Segurança

57. Deve implementar controle de acesso baseado em perfis (Role Based Access Control);
58. Deve implementar VLANs privadas, de forma que permita o isolamento de tráfego de uma porta de acesso das demais portas de acesso de uma mesma VLAN, permitindo acesso apenas para as portas de Uplink (porta promíscua);
59. Deve implementar 802.1x;
60. Deve implementar autenticação baseada em web;
61. Deve implementar autenticação baseada em endereço MAC;
62. Deve permitir a utilização simultânea de autenticação 802.1x e MAC em uma mesma porta;
63. Deve implementar TACACS+. Não serão aceitas soluções similares;
64. Deverá suportar o download de políticas ou ACLsl a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;
65. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam à rede (device profiling) sem a necessidade de agentes instalados nos dispositivos;
66. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo serviços os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, Mac OS e Linux.

Gerenciamento

67. Deve implementar NTP com autenticação MD5;
68. Deve implementar Time Domain Reflectometry (TDR) para testes de cabos UTP, permitindo identificar falhas e verificar a distância do cabo;
69. Deve suportar duas imagens de software na flash;
70. Deve suportar múltiplos arquivos de configuração na flash;
71. Deve permitir o agendamento de tarefas, permitindo executar um comando em um dia e horário específicos;
72. Deve suportar a autoconfiguração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
73. Deve suportar gerenciamento através de plataforma de nuvem do mesmo fabricante, com funcionalidades de gerenciamento de configuração, alertas e notificações e gerenciamento de firmware, sem necessidade de instalação de nenhum software ou dispositivo on-site;
74. Deve suportar IPSec para comunicação com o sistema de gerenciamento;
75. Deve implementar sFlow (IPv4 e IPv6);
76. Deve possuir interface web para configuração;
77. Deve implementar TR-69 (CPE WAN Management Protocol);
78. Deve suportar diagnóstico de transceivers ópticos;
79. Deve implementar Syslog sobre TLS;
80. Deve implementar Secure SFTP (SFTP);
81. Deve implementar SNMP v1/v2/v3;
82. Deve implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) de conexões IP. Deve suportar os seguintes testes: ICMP Echo, UDP-Echo (em porta configurável) e TCP-Connect (em porta configurável) e Jitter UDP para voz;
83. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
84. Deve implementar o isolamento de um Access Point rogue conectado ao switch, quando este for detectado por solução de WLAN do mesmo fabricante;
85. Deve implementar a configuração automática de Access Point wireless do mesmo fabricante quando conectado ao switch. Devem ser suportados os seguintes parâmetros para a configuração automática: VLAN, CoS, largura de banda máxima;
86. Deve suportar o encaminhamento de tráfego para controladora wireless do mesmo fabricante para inspeção e controle de acesso.

Licenciamento

87. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
88. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

Garantia e Suporte

1. O equipamento ofertado deverá possuir garantia do fabricante na modalidade on-site pelo período mínimo de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento. O prazo máximo para atendimento do chamado deve ser de até o próximo dia útil após a sua abertura. Durante o período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis.
2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.
3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de hardware ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;
4. A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.
5. Para efeito de comprovação da garantia, suporte, dos níveis de atendimento e solução exigidos para os equipamentos, deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante a esta deverá ser anexada uma procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.
6. Todos os componentes instalados ou integrados dos equipamentos devem ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 09 – SWITCH DE ACESSO L3 COM 24 PORTAS GIGABIT E 4 SFP+

Características gerais

1. Deve possuir 24 portas 10/100/1000;
2. Deve possuir 4 portas 1/10G SFP+;
3. Deve possuir capacidade de encaminhamento de, no mínimo, 95 Mpps;
4. Deve possuir capacidade de comutação de, no mínimo, 128 Gbps;
5. Deve implementar IEEE 802.3az para as portas 10/100/1000;
6. Deve possuir uma interface de console USB;
7. Deve suportar empilhamento de no mínimo 4 switches;
8. Deve suportar agregação de link através de LACP com no mínimo 20 grupos distribuídos através da pilha, com cada grupo permitindo até 8 portas;
9. Deve suportar a agregação de links entre diferentes membros da pilha;
10. Deve possuir no mínimo 32.000 endereços MAC;
11. Deve possuir latência máxima de 4µs, considerando pacotes de 64 bytes;
12. Deve possuir buffers de, no mínimo, 12 MB;
13. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
14. Deve implementar funcionalidade que permita a detecção de falhas de uplink;
15. Deve implementar no mínimo 2000 VLANs simultaneamente;
16. Deve implementar MVRP (Multiple VLAN Registration Protocol);
17. Deve implementar LLDP (IEEE 802.1ab);
18. Deve implementar LLDP-MED;
19. Deve implementar Q-in-Q (IEEE 802.1ad);
20. Deve implementar PVST+, RPVST+ ou protocolo compatível;
21. Deve implementar MSTP (IEEE 802.1s);
22. Deve implementar túneis VxLAN (VTEP);

Funcionalidades de Camada 3

23. Deve possuir tabela de roteamento com no mínimo 2.000 rotas IPv4 e 1.000 rotas IPv6;
24. Deve implementar roteamento estático;
25. Deve implementar RIP v2, com suporte a autenticação MD5 (RIPv2);

26. Deve implementar RIPng;
27. Deve implementar OSPF;
28. Deve implementar OSPFv3;
29. Deve implementar Policy-based Routing;
30. Deve implementar VRRP;
31. Deve implementar VRRPv3;
32. Deve implementar servidor DHCP;
33. Deve implementar DHCP snooping (IPv4 e IPv6);
34. Deve implementar DHCP relay (IPv4 e IPv6);
35. Deve implementar Gateway mDNS, com suporte a Apple Bonjour;

Multicast

36. Deve implementar PIM-SM;
37. Deve implementar PIM-DM;
38. Deve implementar MLD snooping;
39. Deve implementar IGMP v3;

Software Defined Networking

40. Deve implementar OpenFlow 1.3 ou superior;
41. Deve implementar a separação lógica do tráfego sem suporte a OpenFlow do tráfego com suporte a OpenFlow através de instâncias. O tráfego OpenFlow não pode influenciar o tráfego não openflow no equipamento.
42. Deve permitir configurar cada instância como modo ativo (pacotes referentes a fluxos que o switch não conhece são enviados para a controladora) ou modo passivo (pacotes que não se referem a um fluxo na tabela do switch não são enviados para a controladora)
43. Deve implementar 16 instâncias de OpenFlow;
44. As instâncias de OpenFlow devem suportar a associação de múltiplas VLANs.
45. Cada instância OpenFlow configurada no equipamento deve suportar, pelo menos, a configuração de 3 controladores SDN.
46. Deve permitir utilizar intervalo de portas TCP/UDP e flags de TCP como parâmetros nas regras de OpenFlow;
47. Deve suportar no mínimo 16.000 regras openflow;
48. Deve possuir interface REST API;
49. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE;
50. Deve suportar a criação de VLANs e ACLs no equipamento através de REST.

QoS

51. Deve implementar controle de broadcast;
52. Deve implementar rate limiting para pacotes ICMP;
53. Deve implementar rate limiting para tráfego broadcast e multicast;
54. Deve implementar rate limiting baseado em tráfego classificado por uma ACL;
55. Deve suportar espelhamento de portas;
56. Deve suportar espelhamento de tráfego para um switch remoto.

Segurança

57. Deve implementar controle de acesso baseado em perfis (Role Based Access Control);
58. Deve implementar VLANs privadas, de forma que permita o isolamento de tráfego de uma porta de acesso das demais portas de acesso de uma mesma VLAN, permitindo acesso apenas para as portas de Uplink (porta promíscua);
59. Deve implementar 802.1x;
60. Deve implementar autenticação baseada em web;
61. Deve implementar autenticação baseada em endereço MAC;
62. Deve permitir a utilização simultânea de autenticação 802.1x e MAC em uma mesma porta;

63. Deve implementar TACACS+. Não serão aceitas soluções similares;

64. Deverá suportar o download de políticas ou ACLs a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;

65. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam à rede (device profiling) sem a necessidade de agentes instalados nos dispositivos;

66. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo serviços os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, Mac OS e Linux.

Gerenciamento

67. Deve implementar NTP com autenticação MD5;

68. Deve implementar Time Domain Reflectometry (TDR) para testes de cabos UTP, permitindo identificar falhas e verificar a distância do cabo;

69. Deve suportar duas imagens de software na flash;

70. Deve suportar múltiplos arquivos de configuração na flash;

71. Deve permitir o agendamento de tarefas, permitindo executar um comando em um dia e horário específicos;

72. Deve suportar a autoconfiguração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);

73. Deve suportar gerenciamento através de plataforma de nuvem do mesmo fabricante, com funcionalidades de gerenciamento de configuração, alertas e notificações e gerenciamento de firmware, sem necessidade de instalação de nenhum software ou dispositivo on-site;

74. Deve suportar IPSec para comunicação com o sistema de gerenciamento;

75. Deve implementar sFlow (IPv4 e IPv6);

76. Deve possuir interface web para configuração;

77. Deve implementar TR-69 (CPE WAN Management Protocol);

78. Deve suportar diagnóstico de transceivers ópticos;

79. Deve implementar Syslog sobre TLS;

80. Deve implementar Secure SFTP (SFTP);

81. Deve implementar SNMP v1/v2/v3;

82. Deve implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) de conexões IP. Deve suportar os seguintes testes: ICMP Echo, UDP-Echo (em porta configurável) e TCP-Connect (em porta configurável) e Jitter UDP para voz;

83. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;

84. Deve implementar o isolamento de um Access Point rogue conectado ao switch, quando este for detectado por solução de WLAN do mesmo fabricante;

85. Deve implementar a configuração automática de Access Point wireless do mesmo fabricante quando conectado ao switch. Devem ser suportados os seguintes parâmetros para a configuração automática: VLAN, CoS, largura de banda máxima;

86. Deve suportar o encaminhamento de tráfego para controladora wireless do mesmo fabricante para inspeção e controle de acesso.

Licenciamento

87. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;

88. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

Garantia e Suporte

1. O equipamento ofertado deverá possuir garantia do fabricante na modalidade on-site pelo período mínimo de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento. O prazo máximo para atendimento do chamado deve ser de até o próximo dia útil após a sua abertura. Durante o período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis.

2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.

3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de hardware ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;

4. A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

5. Para efeito de comprovação da garantia, suporte, dos níveis de atendimento e solução exigidos para os equipamentos, deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados. Em caso de

documentação expressa do fabricante a esta deverá ser anexada uma procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.

6. Todos os componentes instalados ou integrados dos equipamentos devem ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 10 – SWITCH DE ACESSO L2 COM 24 PORTAS GIGABIT E 4 SFP

1. Deve possuir 24 portas 10/100/1000;
2. Deve possuir 4 portas 1G SFP;
3. Deve possuir capacidade de encaminhamento de, no mínimo, 40 Mpps;
4. Deve possuir capacidade de comutação de, no mínimo, 56 Gbps;
5. Deve implementar IEEE 802.3az para as portas 10/100/1000;
6. Deve possuir uma interface de console USB;
7. Deve suportar agregação com suporte a até 8 portas por grupo;
8. Deve possuir 16.000 endereços MAC;
9. Deve possuir latência máxima de 4 µs para links de 1000Mbps, considerando pacotes de 64 bytes;
10. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
11. Deve implementar virtual stacking permitindo o gerenciamento de, no mínimo, 16 switches com mesmo endereço IP;
12. Deve implementar 512 VLANs simultaneamente;
13. Deve implementar MVRP (Multiple VLAN Registration Protocol);
14. Deve implementar LLDP (IEEE 802.1ab);
15. Deve implementar LLDP-MED;
16. Deve implementar PVST+, RPVST+ ou protocolo compatível;
17. Deve implementar MSTP (IEEE 802.1s);
18. Deve implementar Gateway mDNS, com suporte a Apple Bonjour;
19. Deve implementar IEEE 802.1p permitindo a classificação de tráfego com até 8 filas de prioridade;
20. Deve permitir a priorização de tráfego por porta e VLAN;
21. Deve implementar controle de broadcast;
22. Deve implementar rate limiting para pacotes ICMP;
23. Deve implementar rate limiting para tráfego broadcast e multicast;
24. Deve suportar espelhamento de portas;
25. Deve implementar RADIUS authentication;
26. Deve implementar RADIUS accounting;
27. Deve implementar TACACS+;
28. Deve implementar IEEE 802.1X com, no mínimo, 8 (oito) autenticações por porta;
29. Deve implementar SSHv2;
30. Deve implementar SSH para IPv6;
31. Deve implementar DHCP snooping;
32. Deve implementar user role localmente permitindo criar políticas de acesso de segurança e QoS, por perfil de usuário e dispositivos;
33. Deve implementar autenticação baseada em web;
34. Deve implementar NTP com autenticação MD5;
35. Deve suportar duas imagens de software na flash;
36. Deve suportar múltiplos arquivos de configuração na flash;
37. Deve permitir o agendamento de tarefas, permitindo executar um comando ou grupo de comandos em um dia e horário específicos;
38. Deve implementar sFlow (IPv4 e IPv6) ou Netflow;
39. Deve implementar RMON com os grupos statistics, history, alarms e events;

40. Deve possuir interface web para configuração;
41. Deve implementar TR-69 (CPE WAN Management Protocol);
42. Deve suportar a auto-configuração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
43. Deve suportar Digital Optical Monitoring (DOM) para transceivers ópticos;
44. Deve implementar Syslog sobre TLS;
45. Deve implementar SFTP ou SCP;
46. Deve implementar SNMP v1/v2/v3
47. Deve permitir gerar notificação caso seja excedido o limite de MACs;
48. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
49. Deve implementar o isolamento de um Access Point rogue conectado ao switch, quando este for detectado por solução de WLAN do mesmo fabricante;
50. Deve implementar a configuração automática de Access Point wireless do mesmo fabricante quando conectado ao switch. Devem ser suportados os seguintes parâmetros para a configuração automática: VLAN, CoS, largura de banda máxima;
51. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
52. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;

Garantia e Suporte

1. O equipamento ofertado deverá possuir garantia do fabricante na modalidade on-site pelo período mínimo de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento. O prazo máximo para atendimento do chamado deve ser de até o próximo dia útil após a sua abertura. Durante o período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis.
2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.
3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de hardware ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;
4. A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.
5. Para efeito de comprovação da garantia, suporte, dos níveis de atendimento e solução exigidos para os equipamentos, deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante a esta deverá ser anexada uma procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.
6. Todos os componentes instalados ou integrados dos equipamentos devem ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 11 – SWITCH DE ACESSO L2 COM 48 PORTAS GIGABIT E 4SFP

1. Deve possuir 48 portas 10/100/1000;
2. Deve possuir 4 portas 1G SFP;
3. Deve possuir capacidade de encaminhamento de, no mínimo, 77 Mpps;
4. Deve possuir capacidade de comutação de, no mínimo, 104 Gbps;
5. Deve implementar IEEE 802.3az para as portas 10/100/1000;
6. Deve possuir uma interface de console USB;
7. Deve suportar agregação com suporte a até 8 portas por grupo;
8. Deve possuir 16.000 endereços MAC;
9. Deve possuir latência máxima de 4 µs para links de 1000Mbps, considerando pacotes de 64 bytes;
10. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
11. Deve implementar virtual stacking permitindo o gerenciamento de, no mínimo, 16 switches com mesmo endereço IP;
12. Deve implementar 512 VLANs simultaneamente;
13. Deve implementar MVRP (Multiple VLAN Registration Protocol);

14. Deve implementar LLDP (IEEE 802.1ab);
15. Deve implementar LLDP-MED;
16. Deve implementar PVST+, RPVST+ ou protocolo compatível;
17. Deve implementar MSTP (IEEE 802.1s);
18. Deve implementar Gateway mDNS, com suporte a Apple Bonjour;
19. Deve implementar IEEE 802.1p permitindo a classificação de tráfego com até 8 filas de prioridade;
20. Deve permitir a priorização de tráfego por porta e VLAN;
21. Deve implementar controle de broadcast;
22. Deve implementar rate limiting para pacotes ICMP;
23. Deve implementar rate limiting para tráfego broadcast e multicast;
24. Deve suportar espelhamento de portas;
25. Deve implementar RADIUS authentication;
26. Deve implementar RADIUS accounting;
27. Deve implementar TACACS+;
28. Deve implementar IEEE 802.1X com, no mínimo, 8 (oito) autenticações por porta;
29. Deve implementar SSHv2;
30. Deve implementar SSH para IPv6;
31. Deve implementar DHCP snooping;
32. Deve implementar user role localmente permitindo criar políticas de acesso de segurança e QoS, por perfil de usuário e dispositivos;
33. Deve implementar autenticação baseada em web;
34. Deve implementar NTP com autenticação MD5;
35. Deve suportar duas imagens de software na flash;
36. Deve suportar múltiplos arquivos de configuração na flash;
37. Deve permitir o agendamento de tarefas, permitindo executar um comando ou grupo de comandos em um dia e horário específicos;
38. Deve implementar sFlow (IPv4 e IPv6) ou Netflow;
39. Deve implementar RMON com os grupos statistics, history, alarms e events;
40. Deve possuir interface web para configuração;
41. Deve implementar TR-69 (CPE WAN Management Protocol);
42. Deve suportar a auto-configuração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
43. Deve suportar Digital Optical Monitoring (DOM) para transceivers ópticos;
44. Deve implementar Syslog sobre TLS;
45. Deve implementar SFTP ou SCP;
46. Deve implementar SNMP v1/v2/v3
47. Deve permitir gerar notificação caso seja excedido o limite de MACs;
48. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
49. Deve implementar o isolamento de um Access Point rogue conectado ao switch, quando este for detectado por solução de WLAN do mesmo fabricante;
50. Deve implementar a configuração automática de Access Point wireless do mesmo fabricante quando conectado ao switch. Devem ser suportados os seguintes parâmetros para a configuração automática: VLAN, CoS, largura de banda máxima;
51. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
52. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

Garantia e Suporte

1. O equipamento ofertado deverá possuir garantia do fabricante na modalidade on-site pelo período mínimo de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento. O prazo máximo para atendimento do chamado deve ser de até o próximo dia útil após a sua abertura. Durante o período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis.
2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.

3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de hardware ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;

4. A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

5. Para efeito de comprovação da garantia, suporte, dos níveis de atendimento e solução exigidos para os equipamentos, deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante a esta deverá ser anexada uma procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.

6. Todos os componentes instalados ou integrados dos equipamentos devem ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 12 – GBIC 10GB PARA ATÉ 300M

Características técnicas mínimas

1. Deve ser do tipo SFP+ de 10GBASE-SR com conector LC;

2. Compatibilidade integral com os Itens 5, 6, 8 e 9.

Garantia e Suporte

3. O equipamento ofertado deverá possuir garantia do fabricante do equipamento na modalidade on-site pelo período mínimo de 12 (doze) meses para reposição de peças, mão de obra e atendimento no local. O período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis;

4. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (part number), incorporado ao equipamento;

5. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 13 – CABO DAC 10GB DE 1M

Características técnicas mínimas

1. Cabo metálico com conector tipo SFP+ para ligação de duas unidades de switch em 10 Gbps;

2. Cabo com comprimento mínimo de 1 (um) metro;

3. Compatibilidade integral com os itens 5, 6, 8 e 9.

Garantia e Suporte

4. O equipamento ofertado deverá possuir garantia do fabricante do equipamento na modalidade on-site pelo período mínimo de 12 (doze) meses para reposição de peças, mão de obra e atendimento no local. O período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis;

5. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (part number), incorporado ao equipamento;

6. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 14 – CABO DAC 10GB DE 3M

Características técnicas mínimas

1. Cabo metálico com conector tipo SFP+ para ligação de duas unidades de switch em 10 Gbps;

2. Cabo com comprimento mínimo de 3 (três) metros;

3. Compatibilidade integral com os itens 5, 6, 8 e 9.

Garantia e Suporte

4. O equipamento ofertado deverá possuir garantia do fabricante do equipamento na modalidade on-site pelo período mínimo de 12 (doze) meses para reposição de peças, mão de obra e atendimento no local. O período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis;

5. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (part number), incorporado ao equipamento;

6. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 15 – GBIC 1GB PARA ATÉ 500M

Características técnicas mínimas

1. Deve ser do tipo SFP de 1G BASE-SX com conector LC;

2. Compatibilidade integral com os Itens 5, 6, 8, 9, 10 e 11.

Garantia e Suporte

3. O equipamento ofertado deverá possuir garantia do fabricante do equipamento na modalidade on-site pelo período mínimo de 12 (doze) meses para reposição de peças, mão de obra e atendimento no local. O período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis;

4. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (part number), incorporado ao equipamento;

5. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 16 – SERVIÇOS DE IMPLANTAÇÃO E TRANSFERÊNCIA DE TECNOLOGIA PARA SWITCHS DE REDE

Características Gerais

1. Os serviços serão realizados em horário de expediente (08:00 às 12:00 e das 14:00 às 18:00) presencialmente no TRE-AL ou remotamente conforme necessidades da CONTRATANTE;

Implantação

2. Instalação e configuração de no mínimo 10 (dez) switchs de rede, contemplando:

3. Configuração básica de acesso a gerencia via rede;

4. Gerencia e monitoramento em **MÓDULO DE GERENCIA DE REDE;**

5. Configuração de autenticação de usuários em **MÓDULO DE CONTROLE DE ACESSO;**

6. Configuração de no mínimo 10 (dez) VLANs;

7. Configuração de stacking de 2 (duas) pilhas com no máximo 4 (quatro) switchs;

8. Configuração de agregação de links em até 10 (dez) switchs com no máximo 4 (quatro) portas por dispositivo.

Transferência de Tecnologia

9. O treinamento deverá ser no realizado na modalidade workshop com tarefas práticas hands-on, visando assim a melhor fixação dos temas abordados com foco direto na explicação da tecnologia dos produtos ofertados como também nas rotinas de configuração, gerenciamento, administração e operação dos mesmos, devendo ter duração mínima de 24 (vinte e quatro) horas onde serão abordados no mínimo os seguintes tópicos:

a. Configuração inicial e acesso a gerencia;

b. Configuração de VLANS;

c. Configuração de autenticação de usuários em **MÓDULO DE CONTROLE DE ACESSO**;

d. Configuração de empilhamento de switchs;

e. Configuração de agregação de links;

f. Configuração de switchs para **MÓDULO DE GERENCIA DE REDE;**

g. Configuração de switchs para **MÓDULO DE ANÁLISE DE TRÁFEGO.**

ITEM 17 - SERVIÇOS DE IMPLANTAÇÃO E TRANSFERÊNCIA DE TECNOLOGIA DO MÓDULO DE CONTROLE DE ACESSO

Características Gerais

1. Os serviços serão realizados em horário de expediente (08:00 às 12:00 e das 14:00 às 18:00) presencialmente no TRE-AL ou remotamente conforme necessidades da CONTRATANTE;

Implantação

2. Instalação e configuração de 1 (uma) instância do serviço controle de acesso, contemplando configurações básicas para acesso à rede, dimensionamento, configuração de armazenamento;

3. Configuração de autenticação em Active Directory para usuários corporativos;

4. Configuração de autenticação de visitantes com portal de autosserviço para criação de usuários;

5. Configuração de no mínimo 10 (dez) dispositivos de rede para autenticação na solução.

Transferência de Tecnologia

6. O treinamento deverá ser no realizado na modalidade workshop com tarefas práticas hands-on, visando assim a melhor fixação dos temas abordados com foco direto na explicação da tecnologia da solução como também nas rotinas de configuração, gerenciamento, administração e operação da mesma devendo ter duração mínima de 24 (vinte e quatro) horas onde será abordado no mínimo os seguintes tópicos:

a. Configuração de Active Directory como base de autenticação;

b. Configuração de autenticação de usuários corporativos;

c. Configuração de autenticação de usuários visitantes;

d. Configuração de portal de autosserviço;

e. Configuração de autenticação e autorização com RADIUS.

ITEM 18 – TREINAMENTO BÁSICO DE ADMINISTRAÇÃO DE SWITCHES

Características Gerais

1. O fornecimento desse item deverá contemplar 01 (um) voucher oficial do fabricante no Treinamento Básico de Administração dos Switches para 01 (um) profissional da contratante;

2. O voucher deverá ter validade de pelo menos 12 (doze) meses;

3. O treinamento deverá ser de acordo com o calendário de treinamento do fabricante e ministrado em centro oficial de treinamento do mesmo ou remotamente, utilizando tecnologia de ensino a distância;

4. Deverá ser ministrado por profissional devidamente credenciado junto ao fabricante e apto a entregar o respectivo;

5. O treinamento deverá compreender a explicação da tecnologia da solução como também das rotinas de configuração, gerenciamento, administração e operação da mesma;

6. O treinamento deverá ter carga horária mínima de 24 (vinte e quatro) horas, ministrado no período de 08:00 às 12:00 e das 14:00 às 18:00.

ITEM 19 – TREINAMENTO BÁSICO DA SOLUÇÃO DE CONTROLE DE ACESSO

Características Gerais

1. O fornecimento desse item deverá contemplar 01 (um) voucher oficial do fabricante no Treinamento da Solução de Controle de Acesso para 01 (um) profissional da contratante;

2. O voucher deverá ter validade de pelo menos 12 (doze) meses;

3. O treinamento deverá ser de acordo com o calendário de treinamento do fabricante e ministrado em centro oficial de treinamento do mesmo ou remotamente, utilizando tecnologia de ensino a distância;

4. Deverá ser ministrado por profissional devidamente credenciado junto ao fabricante e apto a entregar o respectivo;

5. O treinamento deverá compreender a explicação da tecnologia da solução como também das rotinas de configuração, gerenciamento, administração e operação da mesma;

6. O treinamento deverá ter carga horária mínima de 40 (Quarenta) horas, ministrado no período de 08:00 às 12:00 e das 14:00 às 18:00;

LOTE 02 – SOLUÇÃO DE REDE WIRELESS

ITEM 01 – SOLUÇÃO DE ANÁLISE DE PERFIL E CONTROLE DE ACESSO PARA SOLUÇÃO DE REDE WIRELESS

LICENCIAMENTO

1. Licenciamento da **SOLUÇÃO DE ANÁLISE DE PERFIL E CONTROLE DE ACESSO**, contemplando o quantitativo mínimo de 1.000 (um mil) dispositivos, usuários corporativos ou visitantes simultâneos, independente do perfil de autenticação, seja por dispositivo ou usuário;

2. Caso a solução ofertada necessite de licenciamento específico para credenciamento dos dispositivos, usuários (corporativos ou visitantes), deverá ser fornecido o quantitativo solicitado para ambos, de forma que a solução realize a análise de perfil e o controle de acesso dos 1.000 (um mil) dispositivos ou usuários (corporativos ou visitantes) simultâneos.

MÓDULO DE ANÁLISE DE PERFIL DE DISPOSITIVO

Características Gerais Modulo de Análise de Perfil de Dispositivo

3. Deve implementar funcionalidade de classificação automática criando perfis de dispositivos, de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;

4. Deve categorizar os dispositivos em pelo menos 3 níveis:

d. Por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.);

e. Por sistema operacional (ex. Windows, Linux, MacOS, etc.);

f. Versão do sistema operacional (ex. Windows 7, Windows 2008 Server, etc.);

5. Deve ser capaz de gerar gráficos das categorias separando os dispositivos conforme suas características;

6. Deve suportar a coleta de informações, para classificação, usando no mínimo:

k. DHCP;

l. HTTP User-Agent;

m. MAC OUI;

n. ActiveSync plugin;

o. SNMP;

p. Subnet Scanner;

q. IF-MAP;

r. Cisco Device Sensor;

s. MDM;

t. TCP Fingerprinting.

7. Deve possuir dicionário de categorias de dispositivos pré-configurado e mecanismo de atualização do mesmo;

8. Deve suportar a integração com, no mínimo, as seguintes soluções de MDM de mercado AirWatch, MobileIron, BES, JAMF, SOTI, XenMobile, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;

9. Deve permitir priorização na ordem de criação dos perfis com no mínimo as seguintes características:

f. Agente proprietário;

g. HTTP User-Agent;

h. SNMP;

i. DHCP;

j. MAC OUI.

10. A solução de análise de perfil de usuários deverá permitir consultas a sua base, pela solução de controle de acesso para validação de dispositivos com base no seu perfil.

MÓDULO DE CONTROLE DE ACESSO DE DISPOSITIVOS E USUÁRIOS

Características Gerais

11. A Solução deverá dar suporte a no mínimo as seguintes bases de dados:

n. Microsoft Active Directory;

o. Kerberos;

p. Diretórios LDAP;

q. OpenLDAP;

r. PostgreSQL;

s. Oracle 11g;

t. MariaDB;

u. MSSQL;

v. Servidores de Token;

w. Base de dados SQL interna;

x. Lista interna estática de hosts.

12. Deve suportar "Single Sign-on" (SSO) através de SAML v2.0;

13. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

f. Atributos do usuário autenticado;

g. Hora do dia, dia da semana;

h. Tipo de dispositivo utilizado;

i. Localização do usuário;

j. Tipo de autenticação utilizada.

14. Deve permitir a visualização de todas informações relativas a cada transação e autenticação em uma única tela, a solução deverá trazer no mínimo as seguintes informações:

m. Data e Hora;

n. Mac Address do dispositivo;

o. Classificação do dispositivo;

p. Usuário;

q. Equipamento que requisitou a autenticação (origem);

r. Método de autenticação utilizado;

s. Fonte de autenticação utilizada para validação;

t. Perfil de acesso aplicado;

u. Atributos de entrada do protocolo utilizados na requisição (ex. RADIUS);

v. Informações de resposta da solução para o elemento de rede;

w. Alertas em caso de falha;

x. LOGS já filtrados para a requisição em análise.

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

a. a. Lista com últimos Alertas do sistema;

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

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

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

e. Últimas falhas de autenticação;

f. Gráfico com as requisições de avaliação de postura dos dispositivos, divididos em:

- I. Saudáveis (dentro das políticas estabelecidas);

II. Não saudáveis (que estão fora das políticas estabelecidas);

a. a. Lista com as últimas autenticações;

b. Lista com as últimas autenticações com sucesso;

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

16. Deve possuir base de regras e categorias de dispositivos pré-configurada e mecanismo de atualização da mesma;
17. Deve suportar a integração com no mínimo as seguintes soluções de MDM de mercado AirWatch, MobileIron, BES, JAMF, SOTI, XenMobile, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;
18. Deve suportar autenticações via OAuth2, Facebook, Twitter, LinkdIn, Office365 e Google Apps;
19. Deve possuir recursos integrados de AAA: RADIUS, TACACS+ e Kerberos;
20. Deve possuir suporte aos seguintes recursos:

m. RADIUS;

n. RADIUS CoA;

o. TACACS+;

p. Web authentication;

q. SAML v2.0;

r. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);

s. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public);

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

u. EAP-TLS;

v. PAP, CHAP, MSCHAPv1, MSCHAPv2, e EAP-MD5;

w. Windows machine authentication;

x. MAC address authentication (dispositivos sem suporte a 802.1X);

21. Deve suportar verificação de vulnerabilidade através de varredura de portas;
22. Deve suportar à aplicação de políticas em ambiente com múltiplos fornecedores de Wireless, cabeado e VPN;
23. Deve possuir CA integrada, para geração de certificados para os dispositivos que forem se autenticar na rede;
24. Deve suportar à integração com plataforma de terceiros usando HTTP/RESTful API;
25. Deve permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários;
26. Deve possuir suporte a administração através de IPv6;
27. Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilização de usuários visitantes através de portal web seguro;
28. Deve implementar a criação de grupos de autorizadores com privilégios distintos de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;
29. Deve permitir realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;
30. Deve implementar as funcionalidades de geração de lotes de credenciais aleatórias, temporárias, pré-autorizadas;
31. Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;
32. Deve permitir a configuração do tempo de validade das credenciais, baseando-se na criação da conta ou no primeiro login da conta;
33. Deve permitir que o visitante crie sua própria credencial temporária (autosserviço) através de portal web, com ou sem a necessidade de um autorizador;
34. Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante em caso de autosserviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;
35. Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha;
36. Deve exigir que o usuário visitante aceite o “Termo de uso da rede” a cada login ou apenas no primeiro login;
37. Deve permitir o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), e-mail ou impressão local.

GARANTIA E SUPORTE

38. Garantia e suporte do fabricante para a solução de software ofertada pelo período mínimo de 36 (sessenta) meses, incluindo a evolução para novas versões devendo o atendimento ser na modalidade 24x7 (vinte quatro horas por dia, sete dias da semana), com tempo de resposta máximo em 4 (quatro) horas.

39. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.

40. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de software ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;

41. A empresa fabricante da solução de software deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

42. A comprovação da modalidade da garantia deverá ocorrer através de documentação do fabricante de domínio público, não sendo aceita documentação emitida pelo fornecedor ou centro de distribuição para fins de comprovação que por ventura conflitem com catálogos, manuais, folders oficiais impressos ou da internet (devendo constar o endereço URL para folders da web). Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos softwares, indicando o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante deverá ser anexada a mesma a procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.

ITEM 02 – SOLUÇÃO DE GERENCIAMENTO DE REDE WIRELESS

LICENCIAMENTO

1. Deverá ser entregue o quantitativo mínimo de licenças para o gerenciamento simultâneo de 50 (cinquenta) Pontos de acesso;

CARACTERÍSTICAS GERAIS

2. A solução de gerenciamento deverá administrar a configuração dos Pontos de acesso de forma centralizada;

3. A solução de gerenciamento deverá possuir integração com o HPE IMC em console única de gerenciamento;

4. A solução de gerenciamento de rede wireless deverá suportar, em arquitetura de controladora distribuída, a capacidade de gerenciar no mínimo 120 (cento e vinte) pontos de acesso por cluster e no mínimo um total de 20 (vinte) clusters;

5. A solução de gerenciamento, em arquitetura de controladora física ou virtual, deverá suportar no mínimo 2400 pontos de acesso;

6. Deve ser obrigatoriamente do mesmo fabricante dos pontos de acesso e controladores;

7. Permitir a configuração e gerenciamento através de browser padrão (http, https);

8. Permitir que os eventos sejam gravados remotamente utilizando Syslog;

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

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

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

12. Possibilitar a importação de plantas baixas nos formatos dwg e jpg;

13. Permitir a visualização de alertas da rede em tempo real;

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

15. Monitorar o desempenho da rede wireless, consolidando informações de rede tais como:

    a. Níveis de ruído;

    b. Relação sinal-ruído;

    c. Interferência;

    d. Potência de sinal.

16. Possuir capacidade de listagem on-line da localização de usuário, endereço IP, endereço MAC, nível de potência de recepção e dados de associação e de autenticação 802.1x;

17. Deve possuir informação visual e gráfica, na planta baixa dos andares, para:

    a. Visualização dos Pontos de acesso instalados, com estado de funcionamento;

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

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

    d. Localização de Pontos de acesso rogue.

18. Caso esta funcionalidade não esteja disponível no sistema de gerência, deve ser fornecido software, do mesmo fabricante, para atender este item, contemplando todos os dispositivos licenciados e com redundância 1+1;

19. Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID que podem ser percebidos por cada Ponto de acesso;

20. Possuir capacidade de configuração gráfica completa do controlador WLAN seja ela física, virtual ou distribuída e respectivos Pontos de acesso;

21. Possuir capacidade de geração de relatórios dos seguintes tipos:

    a. Listagem de clientes Wireless;

b. Listagem de Pontos de acesso;

c. Informações de Configuração dos Controladores WLAN;

d. Utilização da rede;

e. Detalhes dos Pontos de acesso não autorizados (rogues) detectados.

22. Suportar SSH, HTTP/HTTPS, SSL, Telnet;

23. Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível;

24. Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;

25. Possuir suporte a MIB II, conforme RFC 1213;

26. Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento;

27. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

28. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;

29. Possibilitar a gerência e identificação individualizada de cada Ponto de acesso remoto;

30. Permitir a administração centralizada dos Pontos de acesso sem a necessidade de configurar os mesmos individualmente;

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

32. Possibilitar a importação de plantas baixas nos formatos gráficos (CAD, dwg, jpg, gif e png);

33. Deve disponibilizar em painel gráfico de controle informações referentes à:

a. Sistemas operacionais e tipos de dispositivos que estão se conectando a rede;

b. Informações sobre os tipos de aplicações mais utilizados;

c. Informações sobre usuários conectados.

34. Deve possuir informação sobre possíveis ameaças a rede detectadas pelos sistemas gerenciados;

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

ITEM 03 – LICENÇAS ADICIONAIS PARA SOLUÇÃO DE GERENCIAMENTO DE REDE WIRELESS

Características técnicas mínimas

1. Licença para expansão da **SOLUÇÃO DE GERENCIAMENTO DE REDE WIRELESS**, contemplando o quantitativo adicional mínimo de 1 (um) ponto de acesso simultâneo;

2. Cada unidade deve ser fornecida com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para **SOLUÇÃO DE GERENCIAMENTO DE REDE WIRELESS** especificada nesse edital.

GARANTIA E SUPORTE

1. Garantia e suporte do fabricante para a solução de software ofertada pelo período mínimo de 36 (sessenta) meses, incluindo a evolução para novas versões devendo o atendimento ser na modalidade 24x7 (vinte quatro horas por dia, sete dias da semana), com tempo de resposta máximo em 4 (quatro) horas.

2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.

3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de software ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;

4. A empresa fabricante da solução de software deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

5. A comprovação da modalidade da garantia deverá ocorrer através de documentação do fabricante de domínio público, não sendo aceita documentação emitida pelo fornecedor ou centro de distribuição para fins de comprovação que por ventura conflitem com catálogos, manuais, folders oficiais impressos ou da internet (devendo constar o endereço URL para folders da web). Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos softwares, indicando o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante deverá ser anexada a mesma a procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.

ITEM 04 – LICENCIAMENTO ADICIONAL DA SOLUÇÃO DE ANÁLISE DE PERFIL E CONTROLE DE ACESSO

Características técnicas mínimas

3. Licenciamento para expansão da **SOLUÇÃO DE ANALISE DE PERFIL E CONTROLE DE ACESSO**, contemplando o quantitativo mínimo adicional de 500 (quinhentos) dispositivos, usuários corporativos ou visitantes simultâneos, independente do perfil de autenticação, seja por dispositivo ou usuário;

GARANTIA E SUPORTE

6. Garantia e suporte do fabricante para a solução de software ofertada pelo período mínimo de 36 (sessenta) meses, incluindo a evolução para novas versões devendo o atendimento ser na modalidade 24x7 (vinte quatro horas por dia, sete dias da semana), com tempo de resposta máximo em 4 (quatro) horas.

7. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.

8. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de software ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;

9. A empresa fabricante da solução de software deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

10. A comprovação da modalidade da garantia deverá ocorrer através de documentação do fabricante de domínio público, não sendo aceita documentação emitida pelo fornecedor ou centro de distribuição para fins de comprovação que por ventura conflitem com catálogos, manuais, folders oficiais impressos ou da internet (devendo constar o endereço URL para folders da web). Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos softwares, indicando o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante deverá ser anexada a mesma a procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.

ITEM 05 – CONTROLADORA WLAN

Características gerais

1. Solução baseada em hardware ou software específico, do tipo appliance físico ou virtual, do mesmo fabricante dos pontos de acesso e software de gerência;

2. Deve estar licenciado para controle de, no mínimo, 50 (cinquenta) pontos de acesso, podendo ser expandido em no mínimo, 250 (duzentos e cinquenta) pontos de acesso através de licenciamento adicional;

3. Permitir a conexão simultânea de, no mínimo, 4.000 clientes wireless;

4. Permitir a gravação de eventos por meio do protocolo syslog;

5. Acesso ao sistema através de cliente com browser padrão (http, https, Java);

6. Permitir operação em modo mesh;

7. Permitir o uso de múltiplos SSIDs simultaneamente;

8. Prover tempo de fast-roaming intra-switch inferior a 25 milissegundos;

9. Prover tempo de fast-roaming inter-switch em camada 2, inferior a 100 milissegundos;

10. Permitir conexão entre APs sem a necessidade de conexão cabeada, implementando assim uma rede padrão mesh;

11. Deve suportar 802.11e com WMM, U-APSD e T-SPEC;

12. Gerenciar centralizadamente a autenticação de usuários;

13. Implementar protocolo de autenticação para controle do acesso administrativo a solução com mecanismos de AAA;

14. Possuir base de dados de usuários interna para autenticação de usuários convidados / temporários (acesso guest);

15. Permitir autenticação em no mínimo os seguintes sistemas de base de dados de usuários Microsoft Active Directory, Cisco ACS server, FreeRadius, entre outros;

16. Realizar o provisionamento de usuários convidados (guests) através de interface Web por meio de um usuário administrativo com permissões mínimas, exclusivas para este fim;

17. Possuir suporte a autenticação IEEE 802.1X, com pelo menos os seguintes métodos EAP: EAP-MD5, PEAP/EAP-GTC, PEAP/EAP-MSCHAPv2, EAP-TLS com utilização de base de usuários interna ou servidor RADIUS externo;

18. Suportar as especificações: IEEE 802.1x;

19. Deverá suportar os seguintes métodos EAP-PEAP, EAP-TLS e EAP-TTLS;

20. Possuir suporte a autenticação IEEE 802.1X, com o método PEAP/EAP-GTC, e com utilização de base de usuários LDAP externa;

21. Permitir a seleção/uso de servidor Radius ou LDAP com base no SSID;

22. Suportar a autenticação de usuários conectados à rede cabeada através das portas do controlador;

23. Possuir o recurso de EAP Offload para terminação do túnel EAP no próprio controlador;

24. Deve suportar utilização de Portal Captivo externo ao controlador;
25. Permitir a autenticação (através de endereço MAC, Portal Captivo ou IEEE 802.1X) de usuários conectados à rede WLAN (wireless) ou usuários conectados às portas cabeadas do controlador. Também deverá permitir a autenticação de usuário e de máquina por meio de IEEE 802.1x;
26. Oferecer recurso de Portal Captivo (Captive Portal) com suporte a múltiplos portais simultaneamente;
27. Implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação;
28. Implementar Qualidade de Serviço com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede;
29. Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;
30. Permitir portais captivos externos a controladora;
31. A controladora deve possuir funcionalidade de conexão Site to Site VPN utilizando padrão Ipsec. Caso a solução fornecida não possua a funcionalidade, será aceita solução de VPN adicional integrada;
32. Deve permitir o tunelamento do trafego de dados de usuários mesmo em redes L3, não sendo necessário estender VLANs até o Ponto de Acesso, inclusive em MANs e WANs;
33. Implementar segurança IEEE 802.11i;
34. Suportar a criptografia centralizada com os seguintes protocolos: AES-CCMP, TKIP e WEP;
35. Suportar, no mínimo, 2000 VLANs;
36. Implementar o protocolo 802.1w (Rapid Spanning Tree);
37. Oferecer suporte a roteamento e switching de camadas L2 e L3;
38. Possuir o recurso de criação de Pools de VLAN para permitir a escalabilidade de redes;
39. Possuir servidor DHCP embutido;
40. Suportar o protocolo VRRP para redundância de controladores;
41. Deve suportar redundância de controladores nos modos:
    a. 1+1;
    b. N+1;
    c. Ativo-Ativo;
    d. Ativo-Standby;
42. Oferecer os recursos de mobilidade entre VLANs para roaming de camada 2;
43. Oferecer os recursos de Proxy de endereços IP e Proxy DHCP para roaming entre redes (L3)
44. Deve implementar northbound APIs para realização de integrações com aplicações de terceiros para fins de monitoramento e visibilidade. Caso seja necessário, deve ser ofertado licenças para ativação desse recurso;
45. Implementar tagging de VLANs através do protocolo 802.1Q;
46. Implementar o protocolo 802.1d para Spanning Tree (STP);
47. O controlador WLAN poderá estar diretamente e/ou remotamente conectado aos APs por ele gerenciados, inclusive via roteamento nível 3 da camada OSI
48. Se um controlador WLAN ou AP controlador falhar, os APs relacionados deverão se associar a um controlador WLAN alternativo de forma automática, não permitindo que a rede wireless se torne inoperante;
49. Realizar a descoberta automática dos APs na infraestrutura wireless;
50. Permitir o controle dos APs mediante a conexão através de topologia MESH (WiFi Mesh);
51. A rede MESH deverá oferecer comportamento determinístico da topologia da rede MESH;
52. A rede MESH deverá prover auto-redundância das camadas física (RF) e Layer 2 com comportamento determinístico;
53. Permitir a conexão de APs de maneira remota e segura;
54. Conectar APs através de redes públicas e/ou privadas com garantia de segurança através de conexão criptografada;
55. Permitir a propagação de SSIDs de maneira segura para qualquer AP legitimamente cadastrado na controladora, independentemente de onde este AP esteja conectado;
56. Permitir a autenticação do AP remoto através de certificado digital ou de usuário e senha cadastrados em servidor AD e Radius;
57. Gerenciar o tráfego dos APs centralizadamente;
58. Administrar a configuração dos AP’s;
59. Deve permitir administrar centralizadamente todos os aspectos de segurança da rede WLAN através de firewall integrado à solução de rede sem fio, caso a solução ofertada não possua solução de firewall nativa na controladora WLAN deverá ser ofertado firewall externo com capacidade para atender toda a solução;
60. Permitir o bloqueio de comunicação entre clientes wireless – L2 bridging;
61. Implementar filtros baseados em protocolos e em endereços MAC;

62. Implementar padrão IEEE 802.11h;

63. Realizar o controle de autorização baseado em perfis de acesso;

64. Permitir que seja configurado um perfil de acesso, com regras aplicadas de firewall, para o qual será direcionado o usuário após sua autenticação;

65. Possuir o recurso de “blacklisting” contra ataques ao Firewall e à rede wireless, evitando que um determinado cliente se associe à rede wireless caso viole políticas definidas de Firewall ou execute algum ataque à rede WLAN de endereços MAC de APs do sistema;

66. O Firewall deverá implementar os recursos de NAT (Network Address Translation) tanto para destino quanto para origem;

67. Implementar listas de controle de acesso (ACLs);

68. Oferecer detecção e proteção integrada de ataques de negação de serviços TCP, ICMP;

69. Permitir o espelhamento de sessão e logs detalhados por pacote a fim de possibilitar análises forenses;

70. Permitir a aplicação de políticas de camada 4, de acordo com as características do usuário. Por exemplo, um usuário que pertença ao grupo de gerentes (cadastrado no Radius ou Active Directory) terá permissão de acesso ao protocolo FTP no servidor de ERP;

71. Permitir derivação de políticas de acesso. Por exemplo, um usuário pode pertencer a um grupo ao qual foram atribuídas políticas de acesso em camada 4, porém, caso esteja utilizando um dispositivo de voz, o tráfego SIP passará a ter prioridade através de aplicação de QoS;

72. Permitir a criação de políticas com base em horários e na localização do usuário. Por exemplo: bloquear o tráfego do protocol FTP após às 18 horas.

73. O Firewall deverá ser integrado à rede WLAN de modo a permitir a desassociação de usuários da rede sem fio WLAN com base na violação de políticas de tráfego. Por exemplo: desassociar da rede WLAN e colocar em quarentena o Notebook com endereço MAC XX:XX:XX se o usuário tentar fazer um telnet para o servidor ABC;

74. Otimizar o desempenho e a cobertura da radiofrequência;

75. Ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance;

76. Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura e controle da propagação indesejada de RF;

77. Implementar varredura de RF contínua, programada ou sob demanda, com identificação de APs ou clientes irregulares;

78. Deve implementar a tecnologia de “Channel load balancing”, permitindo que clientes sejam automaticamente distribuídos entre Pontos de Acesso adjacentes operando em canais distintos, com o objetivo de balancear a carga entre os Pontos de Acesso;

79. Deve implementar a tecnologia de “Band Steering/Select”, permitindo que clientes com suporte a faixa de frequência de 5GHz se conectem aos Pontos de Acesso utilizando, preferencialmente, a faixa de 5GHz;

80. Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g, 802.1n e 802.11ac para identificação de ataques e APs intrusos não autorizados (rogues);

81. Realizar a varredura no canal de operação do AP sem impacto na performance da rede WLAN;

82. Permitir a varredura em todos os canais possíveis de RF para detecção e contenção de ameaças na rede WLAN;

83. Deve fazer a varredura dos espectros de 2,4 GHz e 5 GHz para localização e classificação de interferências não 802.11, analise de espectro, e evita-las automaticamente;

84. O controlador deve possuir funcionalidade de analisador gráfico de espectro para detecção de interferências nas faixas de frequência de 2.4 e 5 GHz, sejam elas IEEE 802.11 ou não. Deve disponibilizar interface gráfica com, pelo menos, gráficos de Fast Fourier Transform (FFT) e espectrograma; Caso a funcionalidade não possa ser apresentada pelo controlador, deve ser fornecido um equipamento ou software, do mesmo fabricante, que o faça;

85. Utilizar os APs como ”sensores” de RF para fazer a monitoração do ambiente Wireless;

86. Classificar automaticamente APs válidos, os que interferem e os não autorizados (rogues);

87. Implementar mecanismos para detecção e contenção de APs não autorizados (rogues);

88. Realizar a contenção automática dos APs Rogue, simultaneamente, através da rede WLAN e/ou da rede cabeada;

89. Realizar a identificação e contenção de redes “ad-hoc”;

90. Detectar e bloquear o bridging entre estações da rede WLAN;

91. Oferecer proteção contra ataques Denial Of Service (DOS) a APs e estações

92. Detectar e alertar os seguintes tipos de ataques na rede WLAN:

    a. Impersonalização de AP válido;

    b. Floods de Frames;

    c. Fake Ap, Airjack;

    d. Broadcasts de de-autenticação;

    e. Ataques baseados em probes;

93. Possuir capacidade de gerar alarmes e executar contra-ataques se um ataque for detectado;

94. Detectar áreas de sombra de cobertura e efetuar os devidos ajustes para sua correção, automaticamente;

95. Ajustar, dinamicamente, o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade;

96. Permitir o controle de banda disponível (bandwith contracts) por usuário ou através de perfis de usuários;

97. Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;

98. Deve possuir mecanismo de controle de admissão de chamadas nos pontos de acesso (CAC);

99. Possuir mecanismo automático de QoS para protocolos de voz (SIP, SVP e SCCP) utilizando inspeção automática de pacotes, sem a necessidade de fazer a marcação prévia (tagging) de pacotes;

100. Deve possuir solução de identificação de aplicações através de técnicas de análise de tráfego, provendo informações das aplicações mais utilizadas na interface gráfica;

101. Permitir a criação de políticas de acesso baseadas nas aplicações, como por exemplo, o acesso a “redes sociais” terá um controle de banda de 2Mpbs.

102. Apresentar informações gráficas referente a utilização de soluções de comunicações unificadas (UC) sobre a infraestrutura WLAN, de formar a apresentar informações referentes as chamadas realizadas e relações gráficas entre o nível de sinal recebido pelo usuário e a qualidade da chamada.

103. Possuir a funcionalidade da utilização do protocolo Bonjour na infraestrutura, permitindo que os serviços divulgados via mDNS sejam controlados, filtrados e disponibilizados entre diferentes subnets, tornando assim possível a utilização em redes com múltiplas subnets e um número grande de dispositivos.

104. Cada unidade deve ser fornecida com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis.

Garantia e Suporte

1. O equipamento ofertado deverá possuir garantia do fabricante na modalidade on-site pelo período mínimo de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento. O prazo máximo para atendimento do chamado deve ser de até o próximo dia útil após a sua abertura. Durante o período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis.

2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.

3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de hardware ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;

4. A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

5. Para efeito de comprovação da garantia, suporte, dos níveis de atendimento e solução exigidos para os equipamentos, deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante a esta deverá ser anexada uma procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.

6. Todos os componentes instalados ou integrados dos equipamentos devem ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 06 – LICENÇAS ADICIONAIS PARA CONTROLADORA WLAN

Características técnicas mínimas

3. Licença para expansão da **CONTROLADORA WLAN**, contemplando o quantitativo adicional mínimo de 1 (um) ponto de acesso simultâneo;

4. Deve ser compatível com controladora WLAN especificada nesse edital;

5. Cada unidade deve ser fornecida com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para **CONTROLADORA WLAN** especificada nesse edital.

GARANTIA E SUPORTE

6. Garantia e suporte do fabricante para a solução de software ofertada pelo período mínimo de 36 (sessenta) meses, incluindo a evolução para novas versões devendo o atendimento ser na modalidade 24x7 (vinte quatro horas por dia, sete dias da semana), com tempo de resposta máximo em 4 (quatro) horas.

7. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.

8. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de software ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;

9. A empresa fabricante da solução de software deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

10. A comprovação da modalidade da garantia deverá ocorrer através de documentação do fabricante de domínio público, não sendo aceita documentação emitida pelo fornecedor ou centro de distribuição para fins de comprovação que por ventura conflitem com catálogos, manuais, folders oficiais impressos ou da internet (devendo constar o endereço URL para folders da web). Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos softwares, indicando o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante deverá ser anexada a mesma a procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.

ITEM 07 – PONTO DE ACESSO INTERNO TIPO 01

Características gerais

1. Equipamento de Ponto de Acesso para rede local sem fio, configurável via software, com funcionamento simultâneo nos padrões IEEE 802.11a/n/ac, 5GHz, e IEEE 802.11b/g/n, 2.4GHz;
2. Todos os Pontos de acesso sem fio deverão ser novos e sem nenhum histórico de utilização;
3. Os pontos de acesso deverão possuir certificado emitido pelo “WIFI Alliance” comprovando no mínimo os seguintes padrões, protocolos e funcionalidades:

a. IEEE 802.11a;

b. IEEE 802.11b;

c. IEEE 802.11g;

d. IEEE 802.11n;

e. IEEE 802.11d;

f. IEEE 802.11ac;

g. WPA® Enterprise/Personal;

h. WPA2® Enterprise/Personal;

i. EAP-TLS;

j. EAP-TTLS/MSCHAPv2;

k. PEAPv0/EAP-MSCHAPv2;

l. PEAPv1/EAP-GTC;

m. EAP-SIM;

n. EAP-FAST;

o. WMM® e WMM® Power Save;

p. Beamforming;

q. Short Guard Interval (SGI);

r. Packet Aggregation (A-MPDU);

s. Opportunistic Key Caching (OKC)

4. Deve operar simultaneamente em 2.4GHz e 5GHz (concurrent dual-band);

Performance

5. Deve suportar rádio dual, 5 GHz 802.11ac 2x2 MIMO e 2.4GHz 802.11n 2x2 MIMO
6. Deve suportar capacidade de 1300 Mbps de throughput ou superior;
7. Deve possuir rádio duplo configurável pelo software suportando 5 GHz e 2,4 GHz;
8. Deve possuir no mínimo dois spatial stream Single User (SU) MIMO para taxa de dados sem fio de até 867 Mbps para dispositivos cliente individuais (VHT80) 2x2 em 5GHz;
9. Deve possuir no mínimo dois spatial stream Single User (SU) MIMO para uma taxa de dados sem fio de até 400 Mbps para dispositivos clientes compatíveis (2x2 VHT40) em 5GHz;
10. Deve possuir suporte para até 255 dispositivos cliente associados por rádio e até 16 BSSIDs por rádio;
11. Deve suportar no mínimo as bandas de frequência:

a. 2,400 a 2,4835 GHz

b. 5.150 a 5.250 GHz

c. 5,25 a 5,350 GHz

d. 5,470 a 5,725 GHz

e. 5,725 a 5,850 GHz

12. Deve possuir suporte a seleção de frequência dinâmica (DFS) otimizando o uso do espectro de RF disponível;
13. Deve suportar, no mínimo, as seguintes tecnologias de rádio:

a. 802.11b: espectro espalhável de sequência direta (DSSS)

b. 802.11a/g/n/ac: multiplexação por divisão de frequência ortogonal (OFDM)

14. Deve suportar, no mínimo, os seguintes tipos de modulação:

a. 802.11b: BPSK, QPSK, CCK

b. 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM

15. Deve possuir potência de transmissão configurável em incrementos entre 0,5 e 1,0 dBm.
16. Deve respeitar os limites de potência de transmissão máxima (conduzida):
    a. Faixa de 2,4 GHz: +18 dBm por corrente, agregado de +21 dBm (2x2)
    b. Banda de 5 GHz: +18 dBm por corrente, agregado de +21 dBm (2x2)
17. Deve suportar Advanced Cellular Coexistence (ACC) minimizando a interferência das redes celulares;
18. Deve suportar Maximum ratio combining (MRC) para melhorar o desempenho do receptor;
19. Deve suportar Cyclic delay/shift diversity (CDD/CSD) para melhorar o desempenho RF de downlink;
20. Deve suportar Short guard interval para canais de 20MHz, 40MHz e 80MHz;
21. Deve suportar Space-time block coding (STBC) para aumentar o alcance e melhorar a recepção;
22. Deve suportar Verificação de paridade de baixa densidade (LDPC) para correção de erros de alta eficiência e aumento da taxa de transferência;
23. Deve suportar Transmit beam-forming (TxBF);
24. Deve possuir, no mínimo, as seguintes taxas de dados suportadas (Mbps):
    a. 802.11b: 1, 2, 5.5, 11
    b. 802, 11a / g: 6, 9, 12, 18, 24, 36, 48, 54
    c. 802.11n (2.4GHz): 6.5 a 300 (MCS0 a MCS15)
    d. 802.11ac: 6.5 a 867 (MCS0 a MCS9, NSS = 1 a 2 for VHT20/40/80
25. Deve possuir suporte a 802.11n de alto rendimento (HT): HT 20/40
26. Deve possuir suporte a 802.11ac de alta velocidade (VHT): VHT 20/40/80
27. Deve possuir suporte a agregação de pacotes 802.11n/ac: A-MPDU, A-MSDU

Gerenciamento

28. Deve implementar funcionamento de modo auto gerenciado, sem necessidade de controladora WLAN para configuração de seus parâmetros de rede wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF.
29. Deve obedecer à todas as características descritas mesmo neste modo de funcionamento;
30. No modo de funcionamento auto gerenciado deve disponibilizar na interface gráfica informações de usuários conectados, qualidade de sinal e trafego de dados na rede;
31. O ponto de acesso deve permitir a conversão de modo auto gerenciado para modo gerenciado por controlador WLAN através de interface gráfica, em browser padrão (HTTPS), e permitir que todos os demais pontos de acesso pertencentes ao mesmo cluster, também sejam convertidos automaticamente;
32. O ponto de acesso deverá suportar conexão direta ou remota com controlador WLAN, inclusive via roteamento da camada de rede, baseado no modelo OSI;
33. Se um controlador WLAN falhar, os Pontos de Acesso relacionados deverão se associar automaticamente a um controlador WLAN alternativo, não permitindo que a rede wireless se torne inoperante;
34. Implementar mecanismo de funcionamento para trabalhar com controladores WLAN em redundância;
35. Deve permitir que o ponto de acesso seja atualizado de forma centralizada pela interface gráfica;
36. Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior;
37. Deve possuir servidor DHCP interno configurável;
38. Possibilitar backup e restore da configuração através da interface gráfica;
39. Deve possuir Portal Captivo (Captive Portal) integrado para utilização em rede de visitantes;
40. Deve possuir mecanismos para proteção contra Pontos de Acesso não autorizados (Rogues);
41. Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID;
42. Implementar associação dinâmica de usuários à VLANs com base nos parâmetros da etapa de autenticação;
43. Deve possuir uma base de usuários interna que diferencie usuários visitantes de funcionários, para ser usada em autenticação 802.1x ou portal captivo;
44. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:
    a. MAC Address
    b. 802.1x em base Local
    c. Captive Portal
    d. 802.1x em base externa RADIUS
    e. 802.1x em base externa LDAP

45. Deve permitir a seleção/uso de servidor de autenticação específico com base no SSID;
46. Implementar o protocolo de enlace CSMA/CA para acesso ao meio de transmissão;
47. Possuir capacidade de selecionar automaticamente o canal de transmissão;
48. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF;
49. Permitir habilitar e desabilitar a divulgação do SSID;
50. Implementar diferentes tipos de combinações encriptação/autenticação por SSID;
51. Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;
52. Não deve haver no licenciamento restrições com relação ao número de dispositivos conectados por ponto de acesso;
53. Implementar a pilha de protocolos TCP/IP com suporte a IPV4 e IPV6 (Bridging);
54. Implementar VLANs conforme padrão IEEE 802.1Q;
55. Possuir, no mínimo, uma interface IEEE 802.3 10/100/1000BaseT Ethernet, auto- sensing, auto MDI/MDX;
56. Permitir a atualização remota do sistema operacional e arquivos de configuração através da controladora WLAN
57. Implementar cliente DHCP, para configuração automática de rede;
58. Deve configurar-se automaticamente ao ser conectado na rede;
59. Possuir LED’s indicativos do estado de operação, da atividade do rádio e da interface Ethernet;
60. Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer acessórios para que possa ser feita a fixação;
61. Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de console, cabos de energia elétrica, documentação técnica e manuais (podendo ser em CD-ROM) que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;
62. Permitir o bloqueio da configuração do Ponto de Acesso via rede wireless;
63. Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g, 802.11n, para identificação de Pontos de Acesso intrusos não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede WLAN, sem impacto no seu desempenho;
64. Implementar IEEE 802.1x, com pelo menos os seguintes métodos EAP:
    a. EAP-FAST
    b. EAP-TLS
    c. PEAP-GTC
    d. PEAP-MSCHAPv2
65. Permitir a integração com RADIUS Server com suporte aos métodos EAP citados;
66. A comunicação entre todos os pontos de acesso sem fio e a controladora deverá ser criptografada;
67. Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
68. Implementar WPA com algoritmo de criptografia TKIP e MIC;
69. Implementar WPA2 com algoritmo de criptografia AES, 128/256 bits, IEEE 802.11i;
70. Deve possuir modo dedicado de funcionamento de análise de espectro das faixas de frequência de 2.4 e 5 GHz identificando fontes de interferência nessas faixas;
71. Deve possibilitar analise de espectro nos canais em que estiver provendo acesso, sem desconectar os usuários;
72. Deve disponibilizar informações gráficas de análise de espectro em conjunto com o controlador WLAN;
73. O equipamento deverá possuir registro na ANATEL e deverá ser apresentado na entrega do equipamento;
74. Deverá prover priorização de trafego de vídeo e voz através de parâmetros de QoS (Quality os Service) com possibilidade de aplicar por SSID e dispositivo;
75. Possibilitar roaming na rede wireless;
76. Suportar a criação de uma rede de convidados autocontida com isolamento de tráfego entre clientes e serviços locais;
77. Possuir recursos de seleção automática de canal de transmissão procurando por canais onde haja menor interferência, tendo por objetivo melhorar a performance da rede wireless;
78. Permitir a operação em estrutura Mesh viabilizando a comunicação direta entre diferentes Pontos de Acesso sem Fio onde não seja possível estender a rede cabeada;
79. Operando em estrutura Mesh, a comunicação entre os dispositivos estrutura deverão operar na frequência de 5Ghz.
80. Possuir mecanismo para a restauração das configurações originais de fábrica fisicamente no equipamento (reset);
81. Suportar operação em humidade de 5% a 95% sem condensação;
82. Suportar operação em temperatura de até 40°C (quarenta graus centígrados);
83. Possuir um MTBF (Mean Time Between Failure - Período Médio entre Falhas) de, no mínimo, 250.000 horas.

Garantia e Suporte

1. O equipamento ofertado deverá possuir garantia do fabricante na modalidade on-site pelo período mínimo de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento. O prazo máximo para atendimento do chamado deve ser de até o próximo dia útil após a sua abertura. Durante o período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis.

2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.

3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de hardware ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;

4. A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

5. Para efeito de comprovação da garantia, suporte, dos níveis de atendimento e solução exigidos para os equipamentos, deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante a esta deverá ser anexada uma procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.

6. Todos os componentes instalados ou integrados dos equipamentos devem ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 08 – PONTO DE ACESSO INTERNO TIPO 02

Características gerais

1. Equipamento de Ponto de Acesso para rede local sem fio, configurável via software, com funcionamento simultâneo nos padrões IEEE 802.11a/n/ac, 5GHz, e IEEE 802.11b/g/n, 2.4GHz;

2. Todos os Pontos de acesso sem fio deverão ser novos e sem nenhum histórico de utilização;

3. Os pontos de acesso deverão possuir certificado emitido pelo “WIFI Alliance” comprovando no mínimo os seguintes padrões, protocolos e funcionalidades:

a. IEEE 802.11a;

b. IEEE 802.11b;

c. IEEE 802.11g;

d. IEEE 802.11n;

e. IEEE 802.11d;

f. IEEE 802.11ac;

g. WPA® Enterprise/Personal;

h. WPA2® Enterprise/Personal;

i. EAP-TLS;

j. EAP-TTLS/MSCHAPv2;

k. PEAPv0/EAP-MSCHAPv2;

l. PEAPv1/EAP-GTC;

m. EAP-SIM;

n. EAP-FAST;

o. WMM® e WMM® Power Save;

p. Beamforming;

q. Short Guard Interval (SGI);

r. Packet Aggregation (A-MPDU);

s. Opportunistic Key Caching (OKC)

4. Deve operar simultaneamente em 2.4GHz e 5GHz (concurrent dual-band);

Performance

5. Deve suportar rádio dual, 5 GHz 802.11ac 4x4 MIMO e 2.4 GHz 802.11n 2x2 MIMO;

6. Deve possuir rádio duplo configurável pelo software, suportando 5 GHz e 2,4 GHz;

7. Deve possuir quatro spatial stream Single User (SU) MIMO para taxa de dados sem fio de até 1,733 Mbps, em 5GHz;
8. Deve possuir três spatial stream Multi User (MU) MIMO para uma taxa de dados sem fio de até 1,300 Mbps para dispositivos clientes compatíveis, em 5GHz;
9. Deve possuir suporte para até 255 dispositivos cliente associados por rádio e até 16 BSSIDs por rádio;
10. Deve suportar no mínimo as bandas de frequência:
    a. 2,400 a 2,4835 GHz
    b. 5.150 a 5.250 GHz
    c. 5.250 a 5.350 GHz
    d. 5,470 a 5,725 GHz
    e. 5,725 a 5,850 GHz
11. Deve possuir suporte a seleção de frequência dinâmica (DFS) otimizando o uso do espectro de RF disponível;
12. Deve suportar, no mínimo, as seguintes tecnologias de rádio:
    a. 802.11b: espectro espalhável de sequência direta (DSSS);
    b. 802.11a / g / n / ac: multiplexação por divisão de frequência ortogonal (OFDM);
13. Deve suportar, no mínimo, os seguintes tipos de modulação:
    a. 802.11b: BPSK, QPSK, CCK;
    b. 802.11a / g / n / ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM;
14. Deve possuir potência de transmissão configurável em incrementos de 0,5 dBm;
15. Deve respeitar os limites de potência de transmissão máxima (conduzida):
    a. Faixa de 2,4 GHz: +18 dBm por corrente, agregado de +24 dBm (3x3);
    b. Faixa de 5 GHz: +18 dBm por corrente, agregado de +24 dBm (4x4);
16. Deve suportar Advanced Cellular Coexistence (ACC) minimizando a interferência das redes celulares;
17. Deve suportar Maximum Ratio Combining (MRC) para melhorar o desempenho do receptor;
18. Deve suportar Cyclic delay/shift diversity (CDD/CSD) para melhorar o desempenho RF de downlink;
19. Deve suportar Short guard interval para canais de 20-MHz, 40-MHz e 80-MHz;
20. Deve suportar Space-time block coding (STBC) para aumentar o alcance e melhorar a recepção;
21. Deve suportar verificação de paridade de baixa densidade (LDPC) para correção de erros de alta eficiência e aumento da taxa de transferência;
22. Deve suportar Transmit beam-forming (TxBF);
23. Deve possuir, no mínimo, as seguintes taxas de dados suportadas (Mbps):
    a. 802.11b: 1, 2, 5.5, 11
    b. 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
    c. 802.11n: 6.5 até 450 (MCS0 até MCS23)
    d. 802.11ac: 6.5 até 1,733 (MCS0 até MCS9, NSS = 1 até 4)
24. Deve possuir suporte a 802.11n de alto rendimento (HT): HT 20/40;
25. Deve possuir suporte a 802.11ac de alta velocidade (VHT): VHT 20/40/80;
26. Deve possuir suporte a agregação de pacotes 802.11n/ac: A-MPDU, A-MSDU;

Gerenciamento

27. Deve implementar funcionamento de modo auto gerenciado, sem necessidade de controladora WLAN para configuração de seus parâmetros de rede wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF.
28. Deve obedecer a todas as características descritas mesmo neste modo de funcionamento;
29. No modo de funcionamento autogerenciado deve disponibilizar na interface gráfica informações de usuários conectados, qualidade de sinal e trafego de dados na rede;
30. O ponto de acesso deve permitir a conversão de modo auto gerenciado para modo gerenciado por controlador WLAN através de interface gráfica, em browser padrão (HTTPS), e permitir que todos os demais pontos de acesso pertencentes ao mesmo cluster, também sejam convertidos automaticamente;
31. O ponto de acesso deverá suportar conexão direta ou remota com controlador WLAN, inclusive via roteamento da camada de rede, baseado no modelo OSI;
32. Se um controlador WLAN falhar, os Pontos de Acesso relacionados deverão se associar automaticamente a um controlador WLAN alternativo, não permitindo que a rede wireless se torne inoperante;
33. Implementar mecanismo de funcionamento para trabalhar com controladores WLAN em redundância;

34. Deve permitir que o ponto de acesso seja atualizado de forma centralizada pela interface gráfica;
35. Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior;
36. Deve possuir servidor DHCP interno configurável;
37. Possibilitar backup e restore da configuração através da interface gráfica;
38. Deve possuir Portal Captivo (Captive Portal) integrado para utilização em rede de visitantes;
39. Deve possuir mecanismos para proteção contra Pontos de Acesso não autorizados (Rogues);
40. Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID;
41. Implementar associação dinâmica de usuários à VLANs com base nos parâmetros da etapa de autenticação;
42. Deve possuir uma base de usuários interna que diferencie usuários visitantes de funcionários, para ser usada em autenticação 802.1x ou portal captivo;
43. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:
    a. MAC Address
    b. 802.1x em base Local
    c. Captive Portal
    d. 802.1x em base externa RADIUS
    e. 802.1x em base externa LDAP
44. Deve permitir a seleção/uso de servidor de autenticação específico com base no SSID;
45. Implementar o protocolo de enlace CSMA/CA para acesso ao meio de transmissão;
46. Possuir capacidade de selecionar automaticamente o canal de transmissão;
47. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF;
48. Permitir habilitar e desabilitar a divulgação do SSID;
49. Implementar diferentes tipos de combinações encriptação/autenticação por SSID;
50. Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;
51. Não deve haver no licenciamento restrições com relação ao número de dispositivos conectados por ponto de acesso;
52. Implementar a pilha de protocolos TCP/IP com suporte a IPV4 e IPV6 (Bridging);
53. Implementar VLANs conforme padrão IEEE 802.1Q;
54. Possuir, no mínimo, uma interface IEEE 802.3 10/100/1000BaseT Ethernet, auto- sensing, auto MDI/MDX;
55. Permitir a atualização remota do sistema operacional e arquivos de configuração através da controladora WLAN
56. Implementar cliente DHCP, para configuração automática de rede;
57. Deve configurar-se automaticamente ao ser conectado na rede;
58. Possuir LED’s indicativos do estado de operação, da atividade do rádio e da interface Ethernet;
59. Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer acessórios para que possa ser feita a fixação;
60. Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de console, cabos de energia elétrica, documentação técnica e manuais (podendo ser em CD-ROM) que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;
61. Permitir o bloqueio da configuração do Ponto de Acesso via rede wireless;
62. Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g, 802.11n, para identificação de Pontos de Acesso intrusos não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede WLAN, sem impacto no seu desempenho;
63. Implementar IEEE 802.1x, com pelo menos os seguintes métodos EAP:
    a. EAP- MD5
    b. EAP-FAST
    c. EAP-TLS
    d. PEAP-GTC
    e. PEAP-MSCHAPv2
64. Permitir a integração com RADIUS Server com suporte aos métodos EAP citados;
65. A comunicação entre todos os pontos de acesso sem fio e a controladora deverá ser criptografada;
66. Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
67. Implementar WPA com algoritmo de criptografia TKIP e MIC;

68. Implementar WPA2 com algoritmo de criptografia AES, 128/256 bits, IEEE 802.11i;
69. Deve possuir modo dedicado de funcionamento de análise de espectro das faixas de frequência de 2.4 e 5 GHz identificando fontes de interferência nessas faixas;
70. Deve possibilitar analise de espectro nos canais em que estiver provendo acesso, sem desconectar os usuários;
71. Deve disponibilizar informações gráficas de análise de espectro em conjunto com o controlador WLAN;
72. O equipamento deverá possuir registro na ANATEL e deverá ser apresentado na entrega do equipamento;
73. Deverá prover priorização de trafego de vídeo e voz através de parâmetros de QoS (Quality os Service) com possibilidade de aplicar por SSID e dispositivo;
74. Possibilitar roaming na rede wireless;
75. Suportar a criação de uma rede de convidados autocontida com isolamento de tráfego entre clientes e serviços locais;
76. Possuir recursos de seleção automática de canal de transmissão procurando por canais onde haja menor interferência, tendo por objetivo melhorar a performance da rede wireless;
77. Permitir a operação em estrutura Mesh viabilizando a comunicação direta entre diferentes Pontos de Acesso sem Fio onde não seja possível estender a rede cabeada;
78. Operando em estrutura Mesh, a comunicação entre os dispositivos estrutura deverão operar na frequência de 5Ghz.
79. Possuir mecanismo para a restauração das configurações originais de fábrica fisicamente no equipamento (reset);
80. Suportar operação em humidade de 5% a 95% sem condensação;
81. Suportar operação em temperatura de até 40°C (quarenta graus centígrados);
82. Possuir um MTBF (Mean Time Between Failure - Período Médio entre Falhas) de, no mínimo, 250.000 horas.

Garantia e Suporte

1. O equipamento ofertado deverá possuir garantia do fabricante na modalidade on-site pelo período mínimo de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento. O prazo máximo para atendimento do chamado deve ser de até o próximo dia útil após a sua abertura. Durante o período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis.
2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.
3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de hardware ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;
4. A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.
5. Para efeito de comprovação da garantia, suporte, dos níveis de atendimento e solução exigidos para os equipamentos, deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados. Em caso de documentação expressa do fabricante a esta deverá ser anexada uma procuração que comprove que a fabricante outorga ao procurador os poderes para firmar e declarar as exigências solicitadas.
6. Todos os componentes instalados ou integrados dos equipamentos devem ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 09 – INJETOR POE PARA PONTOS DE ACESSO TIPO 1

Características técnicas mínimas

1. Deve ser do mesmo fabricante dos Pontos de acesso ou homologado e certificado pelo mesmo para utilização em seus equipamentos;
2. Injetor PoE 802.3af 10/100/1000 Ethernet com 15.4W;

Garantia e Suporte

1. O equipamento ofertado deverá possuir garantia do fabricante do equipamento na modalidade on-site pelo período mínimo de 12 (doze) meses para reposição de peças, mão de obra e atendimento no local. O período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis;
2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (part number), incorporado ao equipamento;
3. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 10 – INJETOR POE PARA PONTOS DE ACESSO TIPO 2

Características técnicas mínimas

1. Deve ser do mesmo fabricante dos Pontos de acesso ou homologado e certificado pelo mesmo para utilização em seus equipamentos;
2. Injetor PoE+ 802.3at 10/100/1000 Ethernet com 30W;

Garantia e Suporte

1. O equipamento ofertado deverá possuir garantia do fabricante do equipamento na modalidade on-site pelo período mínimo de 12 (doze) meses para reposição de peças, mão de obra e atendimento no local. O período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis;
2. Caso a garantia padrão do fabricante seja menor que a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (part number), incorporado ao equipamento;
3. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

ITEM 11 – SERVIÇOS DE IMPLANTAÇÃO E TRANSFERÊNCIA DE TECNOLOGIA PARA SOLUÇÃO DE GERENCIAMENTO

Características Gerais

1. Os serviços serão realizados em horário de expediente (08:00 às 12:00 e das 14:00 às 18:00) presencialmente no TRE-AL ou remotamente conforme necessidades da CONTRATANTE;

Implantação

2. Instalação e configuração de 1 (uma) instância do serviço de gerenciamento de rede, contemplando:

a. Configurações básicas para acesso à rede, dimensionamento e configuração de armazenamento;

b. Inclusão de no mínimo 10 (dez) pontos de acesso no monitoramento;

c. Criação de modelo de configuração (templates) de forma a possibilitar a replicação de configuração entre equipamentos.

Transferência De Tecnologia

3. O treinamento deverá ser no realizado na modalidade workshop com tarefas práticas hands-on, visando assim a melhor fixação dos temas abordados com foco direto na explicação da tecnologia da solução como também nas rotinas de configuração, gerenciamento, administração e operação da mesma;

4. O treinamento do **MÓDULO DE GERENCIA DE REDE** deverá ter duração mínima de 24 (vinte e quatro) horas onde será abordado, no mínimo, os seguintes tópicos:

a. Inserção, modificação e remoção de dispositivos de forma unitária e em lote;

b. Configuração de VLANs Globais e Locais em switchs gerenciados;

c. Configuração de ACLS Globais e Locais em switchs gerenciados;

d. Backup e restore de configuração de switchs gerenciados;

e. Monitoramento e alarmes default e customizados;

f. Customização do Dashboard com alertas, mapas de topologia e monitoramento de dispositivos;

ITEM 12 - SERVIÇOS DE IMPLANTAÇÃO E TRANSFERÊNCIA DE TECNOLOGIA DO MÓDULO DE CONTROLE DE ACESSO

Características Gerais

1. Os serviços serão realizados em horário de expediente (08:00 às 12:00 e das 14:00 às 18:00) presencialmente no TRE-AL ou remotamente conforme necessidades da CONTRATANTE;

Implantação

2. Instalação e configuração de 1 (uma) instancia do serviço controle de acesso, contemplando:

a. Configurações básicas para acesso à rede, dimensionamento e configuração de armazenamento;

b. Configuração de autenticação em Active Directory para usuários corporativos;

c. Configuração de autenticação de visitantes com portal de autosserviço para criação de usuários;

d. Configuração de no mínimo 5 (cinco) dispositivos de rede para autenticação na solução.

Transferência de Tecnologia

3. O treinamento deverá ser no realizado na modalidade workshop com tarefas práticas hands-on, visando assim a melhor fixação dos temas abordados com foco direto na explicação da tecnologia da solução como também nas rotinas de configuração, gerenciamento, administração e operação da mesma devendo ter duração mínima de 24 (vinte e quatro) horas onde será abordado no mínimo os seguintes tópicos:

a. Configuração de Active Directory como base de autenticação;

b. Configuração de autenticação de usuários corporativos;

c. Configuração de autenticação de usuários visitantes;

d. Configuração de portal de autosserviço;

e. Configuração de autenticação e autorização com protocolo RADIUS.

ITEM 13 – SERVIÇOS DE IMPLANTAÇÃO E TRANSFERÊNCIA DE TECNOLOGIA PARA CONTROLADORA WLAN E PONTOS DE ACESSO

Características Gerais

1. Os serviços serão realizados em horário de expediente (08:00 às 12:00 e das 14:00 às 18:00) presencialmente no TRE-AL ou remotamente conforme necessidades da CONTRATANTE;

Implantação

2. Instalação e configuração de no mínimo 10 (dez) pontos de acesso, contemplando:

a. Configuração básica de acesso a gerência via rede;

b. Configuração de gerência e monitoramento em **MÓDULO DE GERENCIA DE REDE**;

c. Configuração da autenticação de usuários em **MÓDULO DE CONTROLE DE ACESSO**

d. Configuração de pontos de acesso em controladora WLAN habilitando gerenciamento centralizado;

Transferência de Tecnologia

3. O treinamento deverá ser no realizado na modalidade workshop com tarefas práticas hands-on, visando assim a melhor fixação dos temas abordados com foco direto na explicação da tecnologia dos produtos ofertados como também nas rotinas de configuração, gerenciamento, administração e operação dos mesmos devendo ter duração mínima de 16 (Dezesseis) horas onde será abordado no mínimo os seguintes tópicos:

a. Configuração inicial e acesso a gerência;

b. Configuração de Clusters;

c. Configuração de autenticação de usuários em **MÓDULO DE CONTROLE DE ACESSO**;

d. Criação de SSID com autenticação PSK;

e. Criação de SSID com autenticação enterprise em **MÓDULO DE CONTROLE DE ACESSO;**

f. Configuração de pontos de acesso para **MÓDULO DE GERENCIA DE REDE;**

g. Configuração pontos de acesso para **MÓDULO DE ANÁLISE DE TRÁFEGO;**

ITEM 14 – TREINAMENTO BÁSICO DE ADMINISTRAÇÃO DE ARQUITETURA WLAN

Características Gerais

7. O fornecimento desse item deverá contemplar 01 (um) voucher oficial do fabricante no Treinamento Básico De Administração De Arquitetura Wlan para 01 (um) profissional da contratante;

8. O voucher deverá ter validade de pelo menos 12 (doze) meses;

9. O treinamento deverá ser de acordo com o calendário de treinamento do fabricante e ministrado em centro oficial de treinamento do mesmo ou remotamente, utilizando tecnologia de ensino a distância;

10. Deverá ser ministrado por profissional devidamente credenciado junto ao fabricante e apto a entregar o respectivo;

11. O treinamento deverá compreender a explicação da tecnologia da solução como também das rotinas de configuração, gerenciamento, administração e operação da mesma;

12. O treinamento deverá ter carga horária mínima de 20 (vinte) horas, ministrado no período de 08:00 às 12:00 e das 14:00 às 18:00.

ITEM 15 – TREINAMENTO BÁSICO DA SOLUÇÃO DE GERENCIAMENTO

Características Gerais

1. O fornecimento desse item deverá contemplar 01 (um) voucher oficial do fabricante no Treinamento da Solução de Gerenciamento para 01 (um) profissional da contratante;

2. O voucher deverá ter validade de pelo menos 12 (doze) meses;

3. O treinamento deverá ser de acordo com o calendário de treinamento do fabricante e ministrado em centro oficial de treinamento do mesmo ou remotamente, utilizando tecnologia de ensino a distância;

4. Deverá ser ministrado por profissional devidamente credenciado junto ao fabricante e apto a entregar o respectivo;

5. O treinamento deverá compreender a explicação da tecnologia da solução como também das rotinas de configuração, gerenciamento, administração e operação da mesma;

6. O treinamento deverá ter carga horária mínima de 40 (Quarenta) horas, ministrado no período de 08:00 às 12:00 e das 14:00 às 18:00.

ITEM 16 – TREINAMENTO BÁSICO DA SOLUÇÃO DE CONTROLE DE ACESSO

Características Gerais

7. O fornecimento desse item deverá contemplar 01 (um) voucher oficial do fabricante no Treinamento da Solução de Controle de Acesso para 01 (um) profissional da contratante;

8. O voucher deverá ter validade de pelo menos 12 (doze) meses;

9. O treinamento deverá ser de acordo com o calendário de treinamento do fabricante e ministrado em centro oficial de treinamento do mesmo ou remotamente, utilizando tecnologia de ensino a distância;

10. Deverá ser ministrado por profissional devidamente credenciado junto ao fabricante e apto a entregar o respectivo;

11. O treinamento deverá compreender a explicação da tecnologia da solução como também das rotinas de configuração, gerenciamento, administração e operação da mesma;

12. O treinamento deverá ter carga horária mínima de 40 (Quarenta) horas, ministrado no período de 08:00 às 12:00 e das 14:00 às 18:00.

3.2 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a)

A execução do objeto pressupõe a existência dos seguintes papéis e responsabilidades (Art. 18, § 3º, III, a, 1):

1. Patrocinador da Contratação: é o titular da área demandante, responsável por representar os interesses do órgão no contexto da Contratação, pela aprovação da necessidade e, por fim, pela negociação das ações necessárias para que os objetivos sejam alcançados;
2. Gestor do Contrato (art. 3º, IV, da Resolução TRE/AL nº 15.787/2017): servidor designado para coordenar e comandar o processo da fiscalização da execução contratual. Na forma do Art. 17 da mesma Resolução, o gestor do contrato responsabiliza-se pela condução da gestão e fiscalização do contrato, nos termos do Art. 67, da Lei nº 8.666/93.
3. Fiscal do Contrato (art. 3º, VI, da Resolução TRE/AL nº 15.787/2017): servidor designado para auxiliar o gestor do contrato quanto à fiscalização do objeto do contrato. Neste sentido, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos técnicos da solução.

Dinâmica da Execução (Art. 18, § 3º, III, a, 2):

1. Os equipamentos deverão ser entregues no Almoxarifado do TRE/AL, nos quantitativos indicados no pedido de fornecimento;
2. A garantia dos equipamentos deve obedecer o detalhamento técnico feito e terá seu tempo contado por cada fornecimento individualmente;
3. Entende-se como garantia aquela prestada pelo próprio fabricante ou por rede credenciada pelo fabricante do(s) referido(s) equipamento(s);
4. O pagamento será realizado individualmente para cada nota fiscal apresentada, após emissão do aceite definitivo pela unidade competente do TRE/AL;
5. Os equipamentos deverão ser novos, não recondicionados, de primeiro uso e não deverão conter marcas, amassados, arranhões ou outros problemas e, ainda, serem entregues em pleno estado de funcionamento;
6. Os equipamentos deverão atender rigorosamente a todas as especificações técnicas contidas neste Termo de Referência e em seus Anexos;
7. Os equipamentos deverão vir acompanhados de todos os acessórios necessários para o seu pleno estado de funcionamento, como cabos, drivers, mídias e outros, os quais só serão recebidos juntamente com os respectivos equipamentos. Este item se aplica tanto para a entrega dos equipamentos quanto para substituições durante o período de garantia;
8. Ao TRE é reservado o direito de efetuar conexões dos equipamentos a outros, bem como adicionar demais acessórios compatíveis tecnicamente, sem que isso constitua motivo para a Contratada se desobrigar da garantia, desde que tal fato não implique danos materiais ou técnicos aos equipamentos e acessórios, hipótese que deverá ser devidamente comprovada;
9. Ao TRE/AL é reservado o direito de efetuar diligência, a qualquer tempo, quanto aos documentos exigidos neste Termo de Referência e em seus Anexos.

Recebimento do Objeto:

1. O Tribunal designará Comissão para realizar o recebimento provisório, que só será emitido se os equipamentos estiverem de acordo com as especificações técnicas;
2. Após a entrega, os equipamentos serão submetidos à avaliação e homologação pelos responsáveis técnicos do Tribunal;
3. O exame para comprovação das características técnicas consistirá em avaliações e testes não-destrutivos, por amostragem realizados em duas etapas:
    a. Primeira: inspeção visual de todos os equipamentos entregues;

b. Segunda: testes funcionais de configuração e desempenho, em, no mínimo, 10% (dez por cento) e não menos do que 01 (um) dos equipamentos recebidos. O Tribunal poderá, a seu critério, executar os testes nos demais equipamentos, dentro de um critério de razoabilidade, podendo chegar a 100% dos quantitativos, mas dentro de um prazo máximo de 30 (trinta) dias corridos e contados de cada lote de equipamentos.

4. As especificações serão avaliadas também por meio de documentos técnicos que acompanham os equipamentos, informações fornecidas pela Contratada e disponível no sítio do fabricante.
5. A comissão do Tribunal deverá, após a comprovação do perfeito funcionamento dos equipamentos e adequação às especificações técnicas, emitir e assinar o Termo de Recebimento Definitivo.

Instrumentos Formais de Solicitação do(s) Bens e/ou Serviço(s) (Art. 18, § 3º, III, a, 3):

1. A Ordem de Fornecimento será o instrumento formal de solicitação dos bens pertencentes ao escopo desta contratação.

Forma de Pagamento (Art. 18, § 3º, III, a, 7)

1. O pagamento será efetuado mediante crédito em conta-corrente do Fornecedor, por ordem bancária, no prazo disposto nos artigos 5º, § 3º, ou 40, XIV, "a", da Lei n. 8.666/93, conforme o caso, quando mantidas as mesmas condições iniciais de habilitação e cumpridos os seguintes requisitos:
   a. Apresentação de nota fiscal de acordo com a legislação vigente à época da emissão (nota fiscaleletrônica, se for o caso), acompanhada da Certidão Negativa de Débito – CND, comprovando regularidade com o INSS; do Certificado de Regularidade do FGTS – CRF, comprovando regularidade com o FGTS; da Certidão Conjunta Negativa de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, expedida pela Secretaria da Receita Federal; e da Certidão Negativa de Débitos Trabalhistas – CNDT, emitida pela Justiça do Trabalho; e da prova de regularidade para com as Fazendas Estadual e Municipal do domicílio ou sede do Fornecedor; e
   b. Inexistência de fato impeditivo para o qual tenha concorrido o Fornecedor.
2. Nenhum pagamento será efetuado à Contratada enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária.

Direitos de Propriedade Intelectual (Art. 18, § 3º, III, a, 9):

1. Esse requisito não se aplica ao contexto desta contratação, uma vez que o objeto se refere ao fornecimento de equipamentos, cujos direitos autorais do fabricante são resguardados por legislação nacional e internacional.

Penalidades (Art. 18, § 3º, III, a, 11):

1. Com fundamento no artigo 7º da Lei nº 10.520/2002 e, subsidiariamente, nos artigos 86 e 87 da Lei 8.666/1993, a Contratada ficará sujeita, assegurada prévia e ampla defesa, às seguintes penalidades:
   a. Advertência:
      i. A Contratada será notificada formalmente em caso de descumprimento de obrigação contratual e terá que apresentar as devidas justificativas em um prazo de até 5 (cinco) dias úteis após o recebimento da notificação; e
      ii. Caso não haja manifestação dentro desse prazo ou se entenda serem improcedentes as justificativas apresentadas, a Contratada será advertida;
   b. Multa de:
      i. 0,5% por dia, sobre o valor constante da Ordem de Fornecimento, no caso de atraso injustificado na entrega dos equipamentos, limitada a incidência a 20 (vinte) dias corridos;
         1. No caso de atraso injustificado na entrega dos equipamentos por prazo superior a 20 (vinte) dias corridos, com a aceitação pela Administração, será aplicada a multa de 10% sobre o valor da Ordem de Fornecimento; e
         2. No caso de atraso injustificado na entrega dos equipamentos por prazo superior a 20 (vinte) dias corridos, com a não aceitação pela Administração, será aplicada a penalidade 20% sobre o valor da Ordem de Fornecimento, no caso de inexecução total da obrigação, podendo haver, ainda, o cancelamento do registro de preços do Fornecedor;
      ii. 0,5% por dia, sobre o valor do equipamento, no caso de atraso injustificado na solução do chamado de garantia, limitada a incidência 30 (trinta) dias corridos;
         1. No caso de atraso injustificado na solução do chamado de garantia por prazo superior a 30 (trinta) dias corridos, aplica-se adicionalmente, a multa de 1% sobre o valor da Ordem de Fornecimento; e
         2. A multa por atraso relacionada ao item anterior será auferida por Ordem de Fornecimento e aplicada somente uma única vez a cada mês, independente da quantidade de equipamentos sem solução.
      iii. 10% sobre o valor constante da Ordem de Fornecimento, no caso de inexecução parcial da obrigação assumida;
      iv. 20% sobre o valor da Ordem de Fornecimento, no caso de inexecução total da obrigação, podendo haver, ainda, o cancelamento do registro de preços do Fornecedor;
      v. 10% sobre o valor global estimado da Ata de Ata de Registro de Preços, na hipótese de recusa em assinar a Ata ou o instrumento do contrato, ou retirar a Ordem de Fornecimento.
   c. Impedimento de licitar e contratar com a União e descredenciamento do SICAF pelo prazo de até 5 (cinco) anos, sem prejuízo das demais penalidades legais; e
   d. Declaração de inidoneidade para licitar ou contratar com a Administração Pública.
2. O cometimento reiterado de atrasos injustificados dos prazos previstos para entrega/solução do chamado de garantia dos equipamentos poderá resultar no cancelamento do registro de preços com a Contratada.
3. As sanções previstas nos itens "1.a", "1.c" e "1.d" do item 1 poderão ser aplicadas, cumulativamente ou não, à pena de multa.
4. O valor da multa, aplicada após o regular processo administrativo, será descontado de pagamentos eventualmente devidos à contratada ou cobrado judicialmente;
5. Excepcionalmente, ad cautelam, a Administração poderá efetuar a retenção do valor presumido da multa, antes da instauração do regular procedimento administrativo.

.

4. Requisitos Técnicos (Art. 18, § 3º, IV)

Garantia mínima de 36 (trinta e seis) meses.

Estar comprovadamente ainda em produção.

Conformidade com o presente Termo de Referência.

5. Modelos (templates) propostos a serem utilizados na contratação (Art. 18, § 3º, III, V)

Memorando nº ____ / 20__ - TRE-AL/_____

Maceió, ___ de _____ de _____.

Para: **SGO-COFIN**

Assunto: **Autorização de Emissão de Nota de Empenho.**

PA _____

Adesão à Ata de Registro de Preços _____

Ordem de Fornecimento nº _____/_____.

Senhor Chefe

Encaminhamos estes autos para emissão de **Nota de Empenho,** em favor da **Empresa _____. CNPJ: xx.xxx.xxx/xxxx-xx**, conforme tabela abaixo, tudo em conformidade com o disposto na Resolução TRE-AL nº 12.738/1996 (0216181).

Certidões: SICAF evennto: _____ / RECEITA ESTADUAL evento: _____ / SIMPLES NACIONAL (se aderente) evento: _____

Item:					
Descrição:					
Quant. total da ATA	**Quant. Recebida**	**Quant. desta Ordem**	**Saldo no Fornecedor**	**Valor Unitário**	**Valor Total (R$)**

*** Solicitamos utilizar a reserva de crédito do PE XXX/XXXX**

Gestor da Ata - Portaria TRE/AL nº XX/XXXX

Moodelo a ser adotado em decorrência do comando inserto no Proc SEI nº 0005423-07.2018.6.02.8000, evento 0442132: modelo de referência indicado: 0452895.

Maceió, 15 de maio de 2019.

Documento assinado eletronicamente por **DANIEL MACÊDO DE CARVALHO SOUTO**, **Coordenador**, em 15/05/2019, às 13:36, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-al.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0541748** e o código CRC **1BA26998**.

0008478-63.2018.6.02.8000 0541748v6