



Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Piauí
IFPI
Departamento De Redes E Telecomunicacoes
AV. JÂNIO QUADROS, 330, Santa Isabel, TERESINA / PI, CEP 64053-390
Fone: None Site: www.ifpi.edu.br

TERMO 10/2020 - DRT/DTI/REI/IFPI

TERESINA, 2 de dezembro de 2020.

TERMO DE REFERÊNCIA - CONTRATAÇÕES DE TI

Processo Administrativo nº 23172.001021/2020-28

SOLUÇÃO DE REDE SEM FIO

Histórico de Revisões

Data	Versão	Descrição	Autor
25/06/2020	1.0	Finalização da primeira versão do documento	Benedito Enaldo
08/11/2020	1.1	Adaptação ao PEN-SUAP	Benedito Enaldo
01/12/2020	2.0	Adição de clausulas	Paulo Alex

TERMO DE REFERÊNCIA OU PROJETO BÁSICO

Referência: Arts. 12 a 24 IN SGD/ME Nº 1/2019

1 - OBJETO DA CONTRATAÇÃO

O presente Pregão Eletrônico tem por objeto a aquisição e contratação de empresa especializada no fornecimento de equipamentos (elementos de hardware e software) e serviços em equipamentos de rede, conforme especificações constantes nos artefatos que compõe este processo.

A licitação será dividida em grupos, formados por um ou mais itens, conforme tabela constante no Termo de Referência, facultando-se ao licitante a participação em quantos grupos forem de seu interesse, devendo oferecer proposta para todos os itens que o compõem.

O critério de julgamento adotado será o menor preço GLOBAL do grupo, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

2 - DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1 Bens e serviços que compõem a solução

Lote	Id.	Descrição do Bem ou Serviço	Código CATMAT/CATSER	Quantidade	Métrica ou Unidade
1	1	PONTO DE ACESSO INTERNO	CATMAT - 355896	125	UN
	2	CONTROLADORA DOS PONTOS DE ACESSO	CATMAT - 70653	2	UN
	3	LICENÇAS DE PONTOS DE ACESSO PARA CONTROLADORA	CATSER - 27464	125	UN
	4	INJETOR POE+	CATMAT - 426731	125	UN
	5	SISTEMA DE GERENCIAMENTO	CATSER - 27006	1	UN
	6	LICENÇA PARA SOFTWARE DE GERENCIAMENTO	CATSER - 27464	248	UN
	7	SWITCH DISTRIBUIÇÃO	CATMAT - 466671	8	UN
	8	SWITCH ACESSO 48 PORTAS	CATMAT - 448242	30	UN
	9	SWITCH ACESSO 48 PORTAS POE	CATMAT - 393274	10	UN
	10	SWITCH ACESSO 24 PORTAS	CATMAT - 438620	70	UN
	11	SWITCH ACESSO 24 PORTAS POE	CATMAT - 393274	10	UN
	12	TRANSCEIVER 1G SX	CATMAT - 462023	120	UN
	13	TRANSCEIVER 10G SR	CATMAT - 462024	8	UN
	14	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO	CATSER - 16837	1	UN

3 - JUSTIFICATIVA PARA CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

Nos últimos anos a Tecnologia da Informação tornou-se uma ferramenta fundamental para a execução das principais atividades nos órgãos públicos incluindo também esta Instituição.

Como de praxe, a maioria dos dispositivos tecnológicos, incluindo os ativos de rede, sofrem um processo de depreciação natural que, associado ao avanço das tecnologias, imprime aos gestores a tomada de medidas que garantam a continuidade da prestação de serviços de rede local, da manutenção dos serviços e da prestação de informações de forma eficaz.

A continuidade dos serviços é um dos atributos principais a ser levado em conta pelos gestores já que a interrupção da prestação dos serviços públicos tem potencial de causar transtornos graves aos administrados. Por outro lado, a necessidade de expansão do ambiente de redes de computadores é uma demanda latente do instituto.

Tendo em vista que esta instituição tem um grande impacto quanto à educação pública, qualquer inoperância pode causar um agrave na continuidade de procedimentos que estão correlacionados diretamente e indiretamente a ela.

E para que estas situações sejam proativamente mitigadas, sendo que temos equipamentos que já não possuem mais suporte e atualizações, o instituto opta pela aquisição e expansão dos equipamentos de rede.

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	Objetivos Estratégicos

OE01	Entregar e manter soluções de Tecnologia da Informação alinhadas à estratégia do IFPI
OE02	Aprimorar o atendimento aos usuários do IFPI
OE03	Desenvolver produtos e serviços com celeridade e qualidade
OE04	Aprimorar os processos de governança
OE05	Ampliar a capacidade produtiva
OE10	Adequar infraestrutura para desenvolvimento das ações do IFPI

ALINHAMENTO AO PDTIC			
ID	Ação do PDTIC	ID	Meta do PDTIC Associada
NI.01	Melhoria e ampliação da disponibilidade da cobertura da rede sem fio (Wi-fi), em todos os campi.	M12	Melhorar a Infraestrutura para fornecimento de serviços de TI.
NI.04	Padronização da infraestrutura mínima para os Campus.	M14	Padronizar as soluções de TI utilizadas.
NI.07	Contratação de solução de rede sem fio.	M12	Melhorar a Infraestrutura para fornecimento de serviços de TI.

3.3. Alinhamento aos Instrumentos de Planejamento Institucionais

O Instituto tem constante necessidade de expandir a rede existente, bem como de substituir equipamentos mais antigos, fora de garantia, muito deles já apresentando problemas de funcionamento, como: portas queimadas, sistema de ventilação comprometido e baixa performance em relação à demanda existente.

Frente ao exposto, a Diretoria de Tecnologia da Informação - DTI empreendeu este projeto, em conformidade com a Instrução Normativa nº01, para análise e seleção da melhor solução para atender a demanda de ampliação rede de dados existente.

A estimativa de bens foi elaborada considerando o cenário para a expansão, gerando o seguinte:

Lote	Id.	Descrição	Quantidade
1	1	PONTO DE ACESSO INTERNO	125
	2	CONTROLADORA DOS PONTOS DE ACESSO	2
	3	LICENÇAS DE PONTOS DE ACESSO PARA CONTROLADORA	125
	4	INJETOR POE+	125
	5	SISTEMA DE GERENCIAMENTO	1
	6	LICENÇA PARA SOFTWARE DE GERENCIAMENTO	248
	7	SWITCH DISTRIBUIÇÃO	8
	8	SWITCH ACESSO 48 PORTAS	30
	9	SWITCH ACESSO 48 PORTAS POE	10
	10	SWITCH ACESSO 24 PORTAS	70
	11	SWITCH ACESSO 24 PORTAS POE	10
	12	TRANSCEIVER 1G SX	120
	13	TRANSCEIVER 10G SR	8
	14	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO	1

3.4. Parcelamento da Solução de TIC

A eventual divisão dos objetos da solução em grupos diversos ocasionaria uma situação onde o proponente do item 01, por exemplo, poderia ofertar um equipamento incompatível com os demais componentes desta solução. Para que tal incompatibilidade, entre outras razões, não prejudique os serviços e resultados esperados, a melhor opção é considerar um lote/grupo para cada solução, de acordo com sua característica e especificidade.

Ante ao exposto, é evidente que o agrupamento do objeto, de maneira a compor uma solução unificada, é necessário a fim de evitar eventuais problemas de compatibilidade.

Ademais, lidar com um único fornecedor diminui o custo administrativo de gerenciamento de todo o processo de contratação. O aumento da eficiência administrativa do setor público passa pela otimização do gerenciamento de seus contratos de fornecimento. Essa eficiência administrativa também é de estatura constitucional e deve ser buscada pela administração pública.

Por fim, o agrupamento em lote de todos os equipamentos e softwares visa garantir a otimização dos prazos de execução,

viabilizando a sincronia nos fornecimentos e instalações, evitando assim que um fornecedor venha a prejudicar a execução de outro. Como exemplo mais crítico da situação que se pretende evitar, podemos citar uma situação hipotética na qual o fornecedor do Item 01 tenha problemas na entrega do objeto, isso prejudicará a execução Item 02 já que mesmo instalados os demais itens, estes não serão utilizados de acordo com as suas capacidades até que o Item 01 seja entregue.

3.5. Resultados e Benefícios a Serem Alcançados

LOTE 01: SOLUÇÃO DE REDE SEM FIO

- a. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
- b. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
- c. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet;
- d. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
- e. Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
- f. Renovação dos equipamentos de rede sem fio com qualidade e segurança;
- g. Simplificar a administração dos equipamentos de rede sem fio;
- h. Substituição dos equipamentos da rede sem fio defasados e/ou com defeitos;
- i. Minimização do esforço de aprendizagem por meio da padronização dos equipamentos;
- j. Manter compatibilidade com o software de gerenciamento de pontos de acesso já adquirido;
- k. Garantia da segurança das informações que trafegam pela rede sem fio;
- l. Melhorar a experiência, velocidade e estabilidade na rede sem fio.

4 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

Lote	Id.	Descrição	Quantidade
	1	<p>PONTO DE ACESSO INTERNO</p> <p>1. Equipamento de Ponto de Acesso para rede local sem fio com dois rádios, configurável via software, com funcionamento simultâneo nos padrões IEEE 802.11a/n/ac e ax, 5GHz, e IEEE 802.11b/g/n, 2.4GHz;</p> <p>2. Os pontos de acesso deverão possuir certificado emitido pelo “WIFI Alliance” comprovando os seguintes padrões, protocolos e funcionalidades:</p> <p>2.1. IEEE 802.11a;</p> <p>2.2. IEEE 802.11b;</p> <p>2.3. IEEE 802.11g;</p> <p>2.4. IEEE 802.11n;</p> <p>2.5. IEEE 802.11ac;</p> <p>2.6. IEEE 802.11d</p> <p>2.7. IEEE 802.11h</p> <p>2.8. Wi-Fi Enhanced Open™</p> <p>2.9. WPA2™ - Personal</p> <p>2.10. WPA2™ - Enterprise</p> <p>2.11. WPA3™-Personal</p> <p>2.12. WPA3™-Enterprise</p> <p>2.13. Wi-Fi Vantage™</p> <p>2.14. EAP-SIM;</p>	125

- 2.15. EAP-FAST;
- 2.16. WMM e WMM Power Save;
- 2.17. Short Guard Interval (SGI);
- 2.18. TX A-MPDU.
3. Operar com canais de 20MHz, 40MHz e 80MHz;
4. Atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac, com configuração via software
5. Ser gerenciável pelo controlador WLAN especificado no item 3 para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF
6. Associar-se automaticamente a um controlador WLAN alternativo, não permitindo que a rede wireless se torne inoperante, em caso de falha de um dos controladores WLAN
7. Permitir simultaneamente usuários configurados nos padrões IEEE 802.11b/g/n (2.4GHz) e 802.11a/n/ac (5 GHz), através de rádios independentes (dual radio)
8. Implementar as seguintes taxas de transmissão e com fallback automático
9. IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps
10. IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps
11. IEEE 802.11n: 6.5 a 300 Mbps (MCS0 a MCS15)
12. IEEE 802.11n: 6.5 a 450 Mbps (MCS0 a MCS23), 1 a 3 Spatial Streams
13. IEEE 802.11ac: 6.5 a 1,300 Mbps (MCS0 a MCS9), 1 a 3 Spatial Streams
14. Permitir, no mínimo, 250 (duzentos e cinquenta) usuários simultâneos por rádio
15. Possuir capacidade de selecionar automaticamente o canal de transmissão
16. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF (rádio frequência) conforme as características do ambiente
17. Permitir habilitar e desabilitar a divulgação do SSID
18. Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo
19. Possuir antenas compatíveis com as frequências de rádio dos padrões IEEE 802.11a/b/g/n/ac com padrão de irradiação omnidirecional e tamanho mínimo por antena de:
 - 19.1. 3,9 dBi para 2,4 GHz
 - 19.2. 5,4 dBi para 5,0 GHz
20. Possuir potência máxima de transmissão de, no mínimo:
 - 20.1. 18 dBm no padrão IEEE 802.11a/b/g
 - 20.2. 18 dBm no padrão IEEE 802.11n
 - 20.3. 18 dBm no padrão IEEE 802.11ac
21. Deve possuir sensibilidade de recepção de valor menor ou igual a
 - 21.1. (-74 dBm a 54Mbps no padrão 802.11g
 - 21.2. (-74 dBm a 54Mbps no padrão 802.11a
 - 21.3. (-68 dBm a 450Mbps no padrão 802.11n
 - 21.4. (-58 dBm a 1,300Mbps no padrão 802.11ac
22. Implementar a pilha de protocolos TCP/IP
23. Implementar VLANs conforme padrão IEEE 802.1q
24. Suportar a divulgação e utilização de, no mínimo, 8 (oito) BSSIDs por rádio
25. Possuir, no mínimo, 1 (uma) interface 10/100/1000BaseT Ethernet, auto-sensing, auto MDI/MDX, com conector RJ-45, para transferência de dados com a rede local
26. Permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados no equipamento
27. Possibilitar alimentação elétrica local e via padrão Power over Ethernet (padrão IEEE 802.3af ou 802.3at) através de uma única interface de rede, sem perda de funcionalidades e de desempenho

28. Implementar, em conjunto com o controlador WLAN especificado no item 3, padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps
29. Possuir, em conjunto com o controlador WLAN especificado no item 3, suporte a MIB (Management Information Base)
30. Possibilitar, em conjunto com o controlador WLAN especificado no item 3, a obtenção via SNMP de informações de capacidade e desempenho
31. Implementar cliente DHCP, para configuração automática de rede
32. Suportar os protocolos IPv4 e IPv6 simultaneamente
33. Implementar, em conjunto com o controlador WLAN especificado no item 3, varredura de RF nas bandas 802.11a, 802.11b/g, 802.11n e 802.11ac para identificação de pontos de acesso intrusos não autorizados (rogues access points) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede WLAN, sem impacto no seu desempenho
34. Implementar, em conjunto com o controlador e o software de gerenciamento, mecanismo baseado em VLAN para que usuários não autenticados ganhem acesso restrito na condição de visitante
35. Implementar, em conjunto com o controlador WLAN especificado no item 3, filtros de acesso à rede baseados em endereços MAC
36. Implementar, em conjunto com o controlador WLAN especificado no item 3, IEEE 802.1x, com pelo menos os seguintes métodos: EAP: EAP-TLS, PEAP-MSCHAPv2
37. Permitir, em conjunto com o controlador WLAN especificado no item 3, a integração com Radius Server ou Microsoft Active Directory para autenticação de usuários
38. Implementar, em conjunto com o controlador WLAN especificado no item 3, associação dinâmica de usuário a VLAN, com base nos parâmetros de autenticação
39. Implementar, em conjunto com o controlador WLAN, tunelamento do tráfego remoto, de maneira que o tráfego de determinado SSID seja roteado até a controladora, mesmo que esteja em uma rede remota
40. Implementar, em conjunto com o controlador WLAN, comutação do tráfego local, de maneira que o tráfego de determinado SSID possa ser comutado na rede local sem intervenção da controladora, exceto no aspecto de autenticação dos usuários
41. Implementar, em conjunto com o controlador WLAN, WEP, chaves de 40 bits e 128 bits
42. Implementar, em conjunto com o controlador WLAN, WPA com algoritmo de criptografia TKIP
43. Implementar, em conjunto com o controlador WLAN, WPA2 com algoritmo de criptografia AES, 128 bits
44. Possibilitar o seu gerenciamento através do software de gerenciamento especificado no item 4
45. Possuir certificado válido de homologação emitido pela Anatel
46. Implementar a tecnologia de “Band Steering/Select”, permitindo que clientes se conectem aos Pontos de Acesso utilizando, preferencialmente, a faixa de 5GHz
47. Implementar a tecnologia de “Beam Forming” para melhorar o desempenho de transmissão de dados para determinados usuários da rede sem fio
48. Ser capaz de funcionar nos seguintes modos de operação:
 - 48.1. modo de operação dedicado para atendimento de clientes, simultaneamente nas duas faixas de frequências (2.4GHz e 5GHz)
 - 48.2. modo de operação dedicado como sensor para prevenção de ataques (WIPS), cobrindo todos os canais da faixa de frequências em que o rádio do AP estiver operando (2.4GHz e 5GHz)
 - 48.3. modo de operação combinado em que execute simultaneamente as funções de atendimento de clientes e sensor WIPS, na frequência do canal em que o rádio do AP estiver operando (2.4GHz e 5GHz)

49. Ser capaz de operar, simultaneamente ao atendimento de clientes da rede sem fio, como sensor para análise e varredura de espectro, com resolução mínima de 5MHz, cobrindo todos os canais da faixa de frequências em que o rádio do AP estiver operando (2.4GHz e 5GHz)

50. Possuir antenas internas integradas

51. Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer acessórios para que possa ser feita a fixação

52. Possuir LEDs indicativos do estado de operação do ponto de acesso, do estado de operação de cada rádio e das interfaces Gigabit Ethernet

53. Possuir entrada para dispositivo antifurto;

54. Possuir gerenciamento Inteligente de potência;

55. Deve permitir funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF;

56. Deve permitir funcionamento em modo auto gerenciado, sem a necessidade de uma controladora WLAN, onde o próprio Ponto de Acesso pode operar como um Controladora Virtual:

57. Essa funcionalidade deve ser nativa e não estar atrelada a qualquer tipo de licenciamento adicional;

58. Se uma controladora virtual falhar, os Pontos de Acesso relacionados deverão automaticamente eleger um controlador virtual alternativo, não permitindo que a rede wireless se torne inoperante.

59. Deve permitir temperatura de operação de 0 a 50 graus

60. O equipamento deverá possuir registro na ANATEL;

61. O certificado da ANATEL deverá ser apresentado junto a proposta;

62. Deve fazer parte do catálogo de produtos comercializados pelo fabricante e não constar como: End-of-Support, End-of-Sales e End-of-Life.

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

64. Enquanto o produto estiver em linha de produção, deve ser possível realizar a atualização de software (firmware) dos equipamentos para resolução de problemas de software (correção de bugs);

65. A garantia deve incluir o reparo de peças/equipamentos e reposição enquanto o produto estiver em linha de produção sem nenhum custo à contratante.

66. Deve permitir suporte por telefone ou website para configurações básicas, apenas.

67. Deve fornecer acesso ao website do fabricante para leitura da documentação do equipamento, em caso de necessidade;

68. Deve ser compatível com o sistema de gerenciamento atualmente utilizado pelo IFPI, Airwave;

69. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote).

2 CONTROLADORA DOS PONTOS DE ACESSO

1. Deverá ser fornecido em formato de appliance virtual, compatível com a solução de virtualização VMware ESXi. Caso a solução não seja baseada em máquina virtual, deverão ser fornecidos dois appliance físicos para prover alta disponibilidade;

2. Gerenciar, no mínimo, 150 pontos de acesso, simultaneamente, com centralização das funcionalidades de autenticação;

2

3. Permitir a conexão simultânea de, no mínimo, 800 (oitocentos) clientes wireless;
4. Quando empregado 2 (dois) ou mais controladores, a solução deverá suportar um cenário de alta disponibilidade ativo-ativo, sendo que:
 - 4.1. Deve gerenciar centralizadamente o licenciamento dos pontos de acesso;
 - 4.2. Deve suportar atualizações sem parada total do ambiente, bem como atualização módulos e serviços;
 - 4.3. Deve possuir funcionalidade de otimização de RF baseado em “Machine Learning”;
 - 4.4. Deve suportar balanceamento de carga entre múltiplos controladores;
 - 4.5. Deve ser capaz de gerenciar múltiplas zonas;
 - 4.6. Deve disponibilizar API para integração com ferramentas de terceiros;
 - 4.7. Estas funcionalidades deverão estar habilitadas. Caso seja necessário licenciamento adicional, deverá ser considerado o quantitativo de 50 dispositivos.
5. 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 à queda de alimentação;
6. Permitir gravação de múltiplas configurações no próprio equipamento;
7. Permitir a gravação de eventos por meio do protocolo syslog;
8. Possuir capacidade de gerenciamento hierárquico, com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do grupo sem a necessidade de configuração individual de cada equipamento;
9. Acesso ao sistema através de cliente com browser padrão (http, https);
10. Permitir operação em modo mesh e permitir a utilização de mesh com os pontos de acesso;
11. Permitir o uso de múltiplos SSIDs simultaneamente;
12. Implementar varredura de RF contínua, programada ou sob demanda, com identificação de APs ou clientes irregulares;
13. Na ocorrência de inoperância de um AP, o controlador WLAN deverá ajustar automaticamente a potência dos APs adjacentes, de modo a prover a cobertura da área não assistida;
14. Ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance;
15. Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura e controle da propagação indesejada de RF;
16. Implementar sistema de balanceamento de carga para associação de clientes entre APs próximos, para otimizar a performance;
17. Implementar balanceamento entre APs;
18. Detectar áreas de sombra de cobertura e efetuar os devidos ajustes para sua correção, automaticamente;
19. 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;
20. Permitir o uso de voz e dados sobre um mesmo SSID;
21. Permitir conexão entre APs sem a necessidade de conexão cabeada, implementando assim uma rede padrão mesh;
22. Deve suportar 802.11e com WMM, U-APSD e T-SPEC;
23. Otimizar o desempenho e a cobertura da radiofrequência;
24. Gerenciar de forma centralizada a autenticação de usuários;
25. Administrar de forma centralizada todos os aspectos de segurança da rede WLAN através de firewall integrado à solução de rede sem fio;
26. O controlador deverá oferecer um stateful firewall integrado, baseado em identidade do usuário;

27. Caso o controlador não possua firewall do tipo stateful integrado poderão ser fornecidos appliances, do mesmo fabricante, que contemplem as solicitações e características solicitadas para o firewall;
28. Implementar protocolo de autenticação para controle do acesso administrativo ao equipamento com mecanismos de AAA;
29. Possuir base de dados de usuários interna para autenticação de usuários convidados / temporários (acesso guest);
30. Permitir autenticação em no mínimo os seguintes sistemas de base de dados de usuários Microsoft Active Directory, FreeRadius, entre outros;
31. Realizar o provisionamento de usuários convidados (guests) através de interface Web por meio de um usuário administrativo com permissões mínimas, exclusivas para este fim;
32. Possuir suporte a autenticação IEEE 802.1X, com pelo menos os seguintes métodos: PEAP-GTC, PEAP-MSCHAPv2, EAP-TLS com utilização de base de usuários interna ou servidor RADIUS externo;
33. Suportar as especificações abaixo:
 - 33.1. RFC 2409;
 - 33.2. RFC 2661;
 - 33.3. RFC 2408;
 - 33.4. RFC 3602;
 - 33.5. RFC 3948;
 - 33.6. RFC 2548;
34. Permitir a seleção / uso de servidor Radius ou LDAP com base no SSID;
35. Deve suportar utilização de Portal Captivo externo ao controlador;
36. Permitir a autenticação (através de endereço MAC, Portal Captivo ou IEEE 802.1X) de usuários conectados à rede WLAN (wireless);
37. Oferecer recurso de Portal Captivo (Captive Portal) com suporte a múltiplos portais simultaneamente;
38. Realizar o controle de autorização baseado em perfis de acesso;
39. Permitir que seja configurado um perfil de acesso, com regras aplicadas de firewall, para o qual será direcionado o usuário após sua autenticação;
40. Implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação;
41. Permitir a criação de políticas com base em horários e na localização do usuário. Por exemplo: bloquear o tráfego do protocolo FTP após as 18 horas;
42. Permitir o bloqueio de comunicação entre clientes wireless – L2 bridging;
43. Implementar filtros baseados em protocolos e em endereços MAC;
44. 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;
45. O firewall deverá implementar os recursos de NAT (Network Address Translation) tanto para destino quanto para origem;
46. Implementar listas de controle de acesso (ACLs);
47. Oferecer detecção e proteção integrada de ataques de negação de serviços TCP, ICMP;
48. Permitir o espelhamento de sessão e logs detalhados por pacote a fim de possibilitar análises forenses;
49. 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;
50. Implementar Qualidade de Serviço com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede;

51. Permitir o controle de banda disponível (bandwidth contracts) por usuário ou através de perfis de usuários;
52. Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;
53. Permitir portais cativos externos a controladora;
54. 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;
55. 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;
56. Implementar segurança IEEE 802.11i, além do padrão WPA3;
57. Suportar a criptografia centralizada com os seguintes protocolos: AES-CCMP, TKIP e WEP;
58. Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g, 802.11n e 802.11ac para identificação de ataques e APs intrusos não autorizados (rogues);
59. Realizar a varredura no canal de operação do AP sem desconexão do cliente;
60. Permitir a varredura em todos os canais possíveis de RF para detecção e contenção de ameaças na rede WLAN;
61. Deve fazer a varredura dos espectros de 2,4 GHz e 5 GHz para localização e classificação de interferências não 802.11, análise de espectro, e evita-las automaticamente;
62. 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;
63. Utilizar os APs como “sensores” de RF para fazer a monitoração do ambiente Wireless;
64. Classificar automaticamente APs válidos, os que interferem e os não autorizados (rogues);
65. Implementar mecanismos para detecção e contenção de APs não autorizados (rogues);
66. Realizar o rastreamento e localização física dos APs não autorizados (rogues) utilizando triangulação de rádio frequência;
67. Realizar a contenção automática dos APs Rogue, simultaneamente, através da rede WLAN e da rede cabeada;
68. Realizar a identificação e contenção de redes “ad-hoc”;
69. Detectar e bloquear o bridging entre estações da rede WLAN;
70. Oferecer proteção contra-ataques Denial Of Service (DOS) a APs e estações;
71. Detectar e alertar os seguintes tipos de ataques na rede WLAN:
 - 71.1. Impersonalização de AP válido;
 - 71.2. Floods de Frames;
 - 71.3. Fake Ap, Airjack;
 - 71.4. Broadcasts de autenticação;
 - 71.5. ASLEAP;
 - 71.6. Ataques baseados em probes;
72. Possuir capacidade de gerar alarmes e executar contra-ataques se um ataque for detectado;
73. 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;

74. Implementar o protocolo 802.1w (Rapid Spanning Tree);
75. Oferecer suporte a roteamento e switching de camadas L2 e L3;
76. Suportar as especificações abaixo:
- 76.1. RFC 2328;
- 76.2. RFC 2338;
- 76.3. RFC 1027;
- 76.4. RFC 1519;
77. Possuir o recurso de criação de Pools de VLAN para permitir a escalabilidade de redes;
78. Possuir servidor DHCP embutido;
79. Oferecer os recursos de mobilidade entre VLANs para roaming de camada 2;
80. Implementar tagging de VLANs através do protocolo 802.1Q;
81. O controlador WLAN poderá estar diretamente e/ou remotamente conectado aos APs por ele gerenciados, inclusive via roteamento nível 3 da camada OSI;
82. Permitir o controle de todos os APs mediante a conexão através de topologia MESH (WiFi Mesh);
83. Permitir a conexão de APs de maneira remota e segura;
84. Conectar APs através de redes públicas e/ou privadas com garantia de segurança através de conexão criptografada;
85. Permitir a propagação de SSIDs de maneira segura para qualquer AP legitimamente cadastrado na controladora, independentemente de onde este AP esteja conectado;
86. Permitir a autenticação do AP remoto através de certificado digital ou de usuário e senha cadastrados em servidor AD e Radius;
87. Gerenciar o tráfego dos APs centralizadamente;
88. Administrar a configuração dos AP's;
89. Deve possuir solução de identificação de aplicações através de técnicas de análise de tráfego, provendo informações das aplicações mais utilizadas na interface gráfica;
90. Permitir a criação de políticas de acesso baseadas nas aplicações, como por exemplo, o acesso a "redes sociais" terá um controle de banda de 2 Mbps;
91. Apresentar informações gráficas referente a utilização de soluções de comunicações unificadas (UC) sobre a infraestrutura WLAN, de forma a apresentar informações referentes às chamadas realizadas e relações gráficas entre o nível de sinal recebido pelo usuário e a qualidade da chamada;
92. Deve possuir integração com a solução de firewall utilizada no IFPI, atendendo os seguintes requisitos:
- 92.1. Integração com firewall de próxima geração como: Palo Alto, Fortinet e outros líderes de mercado;
- 92.2. Através da API disponibilizada pelo firewall, deve enviar credenciais de login, tipo de dispositivo, endereço IP e logout;
- 92.3. Estas informações devem permitir ao firewall associar um determinado usuário e dispositivo a uma política definida previamente no firewall.
93. 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;
94. Deve acompanhar suporte do fabricante, incluindo atualizações de versões, pelo período de 3 anos;
95. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote);

3	<p>LICENÇAS DE PONTOS DE ACESSO PARA CONTROLADORA</p> <ol style="list-style-type: none"> 1. Deve adicionar licença de uso de ponto de acesso gerenciados no item Controladora dos pontos de acesso; 2. Deve ser licenciado de forma unitária, permitindo a este órgão adquirir o quantitativo que desejar, respeitando o limite suportado pelo item Controladora dos pontos de acesso; 3. Deve ser obrigatoriamente do mesmo fabricante dos pontos de acesso e controladora dos pontos de acesso; 4. Deve atender na íntegra os requisitos especificados no item Controladora dos pontos de acesso; 5. Deve possuir garantia de suporte de 36 (trinta e seis) meses. Durante este período, para resolução de problemas de software (correção de bugs) e ou problemas com a ativação das licenças; 6. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote). 	125
4	<p>INJETOR POE+</p> <ol style="list-style-type: none"> 1. Injetor PoE (power injector) para alimentação de dispositivos PoE onde não há switch com esta tecnologia; 2. O injetor PoE deverá ser fornecido pelo mesmo fabricante das controladoras e pontos de acesso. Não serão aceitos injetores genéricos e/ou fornecidos por outros fabricantes; 3. Deve permitir o fornecimento de energia conforme o padrão 802.3at, permitindo habilitar todas as funcionalidades dos pontos de acesso; 4. Deve possuir 2 portas RJ-45 fêmea, uma para conectar ao switch não PoE, outra para fornecer energia e dados para o Ponto de Acesso. Ambas as portas devem operar em Gigabit; 5. Deve acompanhar cabos e acessórios para o seu perfeito funcionamento; 6. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V ou 220V com comutação automática e frequência de 60Hz. Deve ser incluído cabo para conexão à rede elétrica no padrão brasileiro; 7. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote); 8. Deve possuir garantia de 12 meses, com substituição do injetor defeituoso em até 21 dias úteis. 	125
5	<p>SISTEMA DE GERENCIAMENTO</p> <ol style="list-style-type: none"> 1. Gerenciar, de maneira centralizada, todos os pontos de acesso, controladores WLAN e switches constantes na solução contratada; 2. Possuir capacidade de expansão futura para suportar no mínimo 512 (quinhentos e doze) pontos de acesso totais; 3. Ser do tipo appliance virtual (arquivo no formato .OVA), totalmente compatível com a solução VMware vSphere 5.5, já utilizada na estrutura de Datacenter virtual do IFPI; 4. Incluir as licenças dos softwares, módulos e dos sistemas operacionais necessários para todos os recursos em caráter permanente, podendo ser utilizadas por tempo indeterminado, mantendo todas as configurações e funcionalidades mesmo após o término da vigência do contrato ou da garantia; 5. Permitir que os eventos sejam redirecionados para servidor de syslog; 	1

6. Possuir capacidade de alteração em lote das características de configuração de um grupo de equipamentos sem a necessidade de configuração individual de cada dispositivo;
7. Permitir acesso ao sistema de gerenciamento por meio de browser padrão via Secure HTTP (HTTPS);
8. Implementar protocolo de autenticação para controle do acesso administrativo da solução utilizando servidor Radius ou Microsoft Active Directory;
9. Implementar recursos de descoberta automática dos dispositivos individuais da infraestrutura wireless;
10. Monitorar o desempenho da rede wireless, consolidando informações de rede tais como: níveis de ruído, relação sinal-ruído, interferência e potência de sinal, permitindo ao administrador isolar e resolver problemas nos vários níveis da rede;
11. Deve permitir a atualização de software dos access points de modo centralizado via navegador;
12. Possibilitar a visualização de informações de clientes conectados à rede sem fio, incluindo as seguintes informações referentes aos clientes de rede sem fio: endereço IP, endereço MAC, nome do usuário, duração da sessão, SSID, canais utilizados, ponto de acesso, controladores aos quais está associado, dados de associação e de autenticação 802.1x;
13. Armazenar informações históricas sobre autenticação de usuários da rede sem fio, tanto da rede corporativa (802.1x) como da rede guest (captive portal);
14. Permitir a localização de endereço IP e de endereço MAC na infraestrutura de rede sem fio;
15. Criar e restaurar backups dos dispositivos gerenciados;
16. Visualizar o histórico dos arquivos de configuração dos dispositivos;
17. Gerar gráficos históricos referentes às seguintes informações: consumo total de rede e número de usuários conectados;
18. Implementar mecanismos para detecção, localização e bloqueio de pontos de acesso não autorizados (rogues);
19. Gerar relatórios com as ameaças de segurança detectadas na rede sem fio;
20. Possuir ferramentas de RF Planning para prever os requerimentos de rádio frequência, permitindo identificar o melhor local para os pontos de acesso na planta do prédio/andar;
21. Deve possuir ferramenta de projeto, realizando cálculo e definição automáticos da quantidade necessária e do posicionamento dos pontos de acesso para que a cobertura desejada nos padrões 802.11g, 802.11n e 802.11ac seja atingida;
22. Permitir a importação de plantas baixas no formato DWG;
23. Permitir ao administrador importar a planta dos andares e assinalar as características de rádio frequência dos pontos de acesso aumentando a precisão do projeto;
24. Disponibilizar mapas gráficos de radiofrequência (heat maps) para apresentar a situação atual do espectro e dos pontos de acesso;
25. Possuir, em conjunto com a controladora, portal de autosserviço que permita que os próprios usuários da rede sem fio visitantes façam a solicitação de acesso por meio de preenchimento de formulários, com possibilidade de aprovação manual realizada por operadores credenciados no sistema;
26. Deve possuir suporte do fabricante pelo período de 36 meses, incluindo: atualização de versão, correção de bugs e suporte remoto ao produto;
27. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote).

6	<p>LICENÇA PARA SOFTWARE DE GERENCIAMENTO</p> <ol style="list-style-type: none"> 1. Deve ser do mesmo fabricante do sistema de gerenciamento; 2. Dever ser fornecida de maneira unitária, para fins de volumetria considerar 1 (um) dispositivo equivale a 1 (uma) licença; 3. A licença deve permitir o gerenciamento de forma completa do dispositivo alvo; 4. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote); 5. Deve ser fornecido com garantia de 36 (trinta e seis) meses; 6. Deve permitir suporte por telefone ou website para configurações; 7. Deve fornecer acesso ao website do fabricante para leitura da documentação do equipamento, em caso de necessidade. 	248
7	<p>SWITCH DISTRIBUIÇÃO</p> <ol style="list-style-type: none"> 1. Deve permitir instalação em rack de 19” padrão Telco EIA; 2. Deve possuir altura máxima 1 (um) rack unit (RU); 3. Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC; 4. Deve possuir slot para fonte de alimentação interna, redundante, do tipo auto-sense, para operar de 100 a 240 VAC; 5. Deve possuir 24 (vinte e quatro) portas 10/100/1000BASE-T, usando conectores RJ-45; 6. As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático; 7. Deve possuir no mínimo 04 portas SFP/SFP+, 1/10GBASE-X que suportem transceivers com conectores SC ou LC; 8. As portas SFP/SFP+ devem suportar, no mínimo, as seguintes interfaces SFP+: 10GBASE-SR, LR, LRM e ER e interfaces SFP: 1GBASE-SX,LX e T, que não devem operar em modo “combo” com as portas 10/100/1000 BASE-T em par trançado; 9. Deve suportar capacidade de processamento igual ou superior a 190 (noventa e cinco) Mpps; 10. Deve suportar capacidade de switching igual ou superior a 320 (Cento e sessenta) Gbps; 11. Deve possuir pelo menos 13 MB de buffers de pacotes; 12. Deve possuir pelo menos 2 GB de memória DRAM; 13. Deve implementar a tecnologia de empilhamento com outra unidade switch de mesmo fabricante, tomando esse empilhamento uma única unidade de encaminhamento L3 e L2 ininterrupto e gerenciamento de múltiplos dispositivos por um único IP. Esta agregação deverá ser feita através de 2 (duas) portas físicas, dedicadas para esta função, ou podendo ser utilizadas as interfaces SFP+, desde que não seja as portas do item 8 acima. 14. Deve permitir empilhamento de no mínimo 09 (nove) unidades. As licenças e módulos necessários para empilhamento devem ser fornecidos; 15. O equipamento deve ser acompanhado do cabo de empilhamento com comprimento mínimo de 1 metro; 16. Deve suportar banda agregada de empilhamento mínima de 20 (vinte) Gbps, utilizando duas portas de 10 (dez) Gbps; 17. Deve suportar banda agregada de empilhamento mínima de 40 (quarenta) Gbps, utilizando quatro portas de 10 (dez) Gbps; 18. Deve suportar a criação de grupos de agregação de link contendo portas em unidades 	8

diferentes da pilha;

19. Deve implementar agregação de links em modo estático e dinâmico (LACP), com suporte a criação de até 128 grupos. Deve ser possível a formação de grupos com 8 portas Gigabit e grupos com 8 portas 10Gbps;

20. Deve suportar porta de gerenciamento “out-of-band” operando a 10/100/1000 Mbps;

21) Deve suportar porta de console para gerenciamento utilizando conector RJ45 ou micro usb;

22. Deve suportar certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet;

Funções de Camada 2

23. Deve suportar capacidade de no mínimo 64.000 (sessenta e quatro mil) endereços MAC;

24. A pilha deve suportar capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad;

25. Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 vlans ativas;

26. Deve implementar o protocolo IEEE 802.1D (Spanning Tree Protocol);

27. Deve implementar o protocolo IEEE 802.1w (Rapid Spanning Tree);

28. Deve implementar os protocolos IEEE 802.1s (MSTP) para criação de , no mínimo, 64 instâncias de Spanning Tree;

29. Deve implementar Spanning Tree BPDU Protection (BPDU Guard);

30. Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;

31. Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão 802.1ad ou similar;

32. Deve implementar o protocolo UDLD (Uni-Directional Link Detection) ou similar;

33. Deve implementar jumbo frames até 9000 bytes em todas as portas;

34. Deve implementar mecanismos para controle de tráfego unknown, unicast, broadcast e multicast;

35. Deve implementar GVRP, MVRP ou similar;

Funções de Camada 3

36. Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;

37. Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;

38. Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPng;

39. Deve implementar OSPF, OSPFv3, BGP4, BGP4+;

40. Deve implementar Proxy ARP;

41. Deve suportar RFC 2328 OSPFv2;

42. Deve implementar RFC 3101 OSPF NSSA;

43. Deve implementar BFD;

44. Deve suportar capacidade de pelo menos 10.000 (dez mil) entradas na tabela de roteamento IPv4;

45. Deve suportar capacidade de pelo menos 5000 (cinco mil) entradas na tabela de roteamento Ipv6;

46. Deve implementar Equal-Cost Multipath (ECMP);

47. Deve implementar PIM-DM, PIM-SM, MLDv2 e MLD v2 snooping tanto em IPv4 e IPv6;

48. Deve implementar roteamento baseado em políticas (Policy-Based routing);

49. Deve implementar VRRP;

50. Deve implementar autenticação MD5 para RIP e OSPF;

Qualidade de Serviço;

51. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;

52. Suportar QoS nas seguintes funcionalidades: priorização IEEE 802.1p COS, prevenção de congestionamento (WRED/RED) e gerenciamento de filas (Strict Priority, WRR e WFQ) ou similares;

53. Permitir a classificação, marcação e priorização de pacotes IP utilizando DSCP (Differential, Services Code Point) para L3 e TOS (Type Of Service) para L2;

54. Implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;

55. Deve permitir a configuração de Rate Limiting de entrada;

56. Deve permitir a configuração de Rate Shaping ou Rate limiting de saída;

Segurança

57. Deve suportar protocolos para proteção de ataques de Denial of Service;

58. Deve implementar proteção contra ataques de ARP;

59. Deve implementar proteção contra IP spoofing (IP source guard);

60. Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando perfis definidas por um servidor RADIUS externo;

61. Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;

62. Implementar método de autenticação baseado em endereço MAC para os dispositivos que não suportarem suplicantes 802.1X;

63. Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;

64. Deve implementar listas de controle de Acesso (ACL) baseado em baseada em endereço IPv4, IPv6 e MAC de origem e destino, porta protocolo;

65. Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;

65.1. Deve permitir a criação de filtros de endereço MAC de origem e destino;

66. Implementar DHCP snooping e DHCPv6 snooping;

67. Deve suportar o isolamento de portas, de forma que uma porta isolada não possa enviar tráfego para outra porta isolada do mesmo switch, mesmo que estejam na mesma VLAN;

68. Deve implementar funcionalidade que permita que a configuração de root do Spanning Tree seja mantida mesmo no caso de recebimento de BPDU com maior prioridade (root guard);

69. Deve implementar SSL;

70. Deve implementar a configuração de limites para tráfego broadcast e multicast por porta. Casca; limites configurados sejam excedidos, deve ser possível desabilitar a porta;

71. Deve implementar RFC 2865 Remote Authentication Dial In User Service (RADIUS);

72. Deve implementar RFC 2866 RADIUS Accounting;

Gerenciamento

73. Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;

74. Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;
75. Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;
76. Deve permitir espelhamento de tráfego por porta e baseado em ACL;
77. Deve implementar espelhamento remoto com destino a outro switch na mesma rede L2;
78. Deve implementar gerenciamento usando SSH v2. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
79. Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
80. Deve implementar pelo menos 4 (quatro) grupos de RMON;
81. Deve implementar Xmodem e TFTP;
82. Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
83. Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB;
84. Deve implementar o protocolo OpenFlow 1.3 com suporte para portas híbridas em Camada 2 e Camada 3;
85. Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;
86. Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP ou SNTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
87. Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash;
88. Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve v6 para a funcionalidade solicitada ;
89. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE”;
90. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote);

Licenciamento

91. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
92. 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

93. Deve possuir garantia enquanto o produto estiver em linha de fabricação.
94. O fabricante deverá enviar um equipamento novo, em caso de falha do adquirido na modalidade NBD pelo período de 36 meses.
95. Deve permitir suporte por telefone ou website para configurações básicas, apenas.
96. Deve fornecer acesso ao website do fabricante para leitura da documentação do equipamento, em caso de necessidade;

1. Deve possuir 48 portas 10/100/1000;
2. Deve possuir 4 portas 1 GbE 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 possuir uma interface de console USB;
6. Deve prover endereçamento IP para o gerenciamento de até 16 switches individualmente;
7. Deve suportar agregação de link através de LACP;
8. Deve possuir 16.000 endereços MAC;
9. Deve possuir latência máxima de 3 μ s, considerando pacotes de 64 bytes nas interfaces 1 GbE;
10. Deve suportar sflow através da RFC 3176;
11. Deve possuir buffers de, no mínimo, 1,5 MB;
12. Deve implementar 512 VLANs simultaneamente;
13. Deve implementar LLDP (IEEE 802.1ab);
14. Deve implementar LLDP-MED;
15. Deve implementar PVST+, RPVST+ ou protocolo compatível;
16. Deve implementar MSTP (IEEE 802.1s);
17. Deve implementar MLD snooping;
18. Deve implementar IGMP v3;
19. Deve suportar espelhamento de portas;
20. Deve implementar 802.1x;
21. Deve implementar autenticação baseada em web;
22. Deve implementar autenticação baseada em endereço MAC;
23. Deve implementar TACACS+. Não serão aceitas soluções similares;
24. Deve implementar SNMP;
25. Deve suportar duas imagens de software na memória flash;
26. Deve suportar múltiplos arquivos de configuração na memória flash;
27. Deve implementar sFlow (IPv4 e IPv6);
28. Deve possuir interface web para configuração;
29. Deve implementar TR-069;
30. Deve implementar Syslog;
31. Deve implementar nativamente 4 (quatro) grupos RMON (Estatísticas, Históricos, Alarmes e Eventos)
32. Deve implementar Secure FTP (SFTP);
33. Deve implementar SNMP v1/v2/v3;
34. O equipamento não pode constar na lista de produtos e com anúncio de end-of sales pelo fabricante;
35. Deve possuir interface REST API ;
36. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
37. Deve implementar o isolamento de um Access Point rogue conectado ao switch, quando este for detectado por solução de WLAN do mesmo fabricante;

38. 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;

39. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE”;

40. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote);

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

Licenciamento

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

43. 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

44. Deve possuir garantia enquanto o produto estiver em linha de fabricação.

45. O fabricante deverá enviar um equipamento novo, em caso de falha do adquirido na modalidade NBD pelo período de 36 meses.

46. Deve permitir suporte por telefone ou website para configurações básicas, apenas.

47. Deve fornecer acesso ao website do fabricante para leitura da documentação do equipamento, em caso de necessidade.

9 SWITCH ACESSO 48 PORTAS POE

10

1. Deve possuir 48 portas 10/100/1000;
2. Deve possuir 4 portas 1 GbE SFP;
3. Deve possuir capacidade de encaminhamento de, no mínimo, 77.3 Mpps;
4. Deve possuir capacidade de comutação de, no mínimo, 104 Gbps;
5. Deve implementar PoE+ (IEEE 802.3at) em cada porta 10/100/1000BaseT. A fonte interna do switch deve disponibilizar 380W de potência para alimentação do conjunto de portas PoE+;
6. Deve possuir uma interface de console USB;
7. Deve prover endereçamento IP para o gerenciamento de até 16 switches individualmente;
8. Deve suportar agregação de link através de LACP;
9. Deve possuir 16.000 endereços MAC;
10. Deve possuir latência máxima de 3 µs, considerando pacotes de 64 bytes nas interfaces 1 GbE;
11. Deve suportar sflow através da RFC 3176;
12. Deve possuir buffers de, no mínimo, 1.5 MB;
13. Deve implementar 512 VLANs simultaneamente;
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 MLD snooping;
19. Deve implementar IGMP v3;
20. Deve suportar espelhamento de portas;
21. Deve implementar 802.1x;
22. Deve implementar autenticação baseada em web;
23. Deve implementar autenticação baseada em endereço MAC;
24. Deve implementar TACACS+. Não serão aceitas soluções similares;
25. Deve implementar SNMP;
26. Deve suportar duas imagens de software na memória flash;
27. Deve suportar múltiplos arquivos de configuração na memória flash;
28. Deve implementar sFlow (IPv4 e IPv6);
29. Deve possuir interface web para configuração;
30. Deve implementar TR-069;
31. Deve implementar Syslog;
32. Deve implementar nativamente 4 (quatro) grupos RMON (Estatísticas, Históricos, Alarmes e Eventos)
33. Deve implementar Secure FTP (SFTP);
34. Deve implementar SNMP v1/v2/v3;
35. O equipamento não pode constar na lista de produtos e com anúncio de end-of sales pelo fabricante;
36. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
37. Deve implementar o isolamento de um Access Point rogue conectado ao switch, quando este for detectado por solução de WLAN do mesmo fabricante;
38. 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, potência PoE e prioridade PoE;
39. Deve possuir interface REST API;
40. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE”;
41. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote);
42. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;

Licenciamento

43. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
44. 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

45. Deve possuir garantia enquanto o produto estiver em linha de fabricação.
46. O fabricante deverá enviar um equipamento novo, em caso de falha do adquirido na modalidade NBD pelo período de 36 meses.

- 47. Deve permitir suporte por telefone ou website para configurações básicas, apenas.
- 48. Deve fornecer acesso ao website do fabricante para leitura da documentação do equipamento, em caso de necessidade.

10 SWITCH ACESSO 24 PORTAS

70

- 1. Deve possuir 24 portas 10/100/1000;
- 2. Deve possuir 4 portas 1 GbE SFP;
- 3. Deve possuir capacidade de encaminhamento de, no mínimo, 41 Mpps;
- 4. Deve possuir capacidade de comutação de, no mínimo, 56 Gbps;
- 5. Deve possuir uma interface de console USB;
- 6. Deve prover endereçamento IP para o gerenciamento de até 16 switches individualmente;
- 7. Deve suportar agregação de link através de LACP;
- 8. Deve possuir 16.000 endereços MAC;
- 9. Deve possuir latência máxima de 3 μ s, considerando pacotes de 64 bytes nas interfaces 1 GbE;
- 10. Deve suportar sflow através da RFC 3176;
- 11. Deve possuir buffers de, no mínimo, 1.5 MB;
- 12. Deve implementar 512 VLANs simultaneamente;
- 13. Deve implementar LLDP (IEEE 802.1ab);
- 14. Deve implementar LLDP-MED;
- 15. Deve implementar PVST+, RPVST+ ou protocolo compatível;
- 16. Deve implementar MSTP (IEEE 802.1s);
- 17. Deve implementar MLD snooping;
- 18. Deve implementar IGMP v3;
- 19. Deve suportar espelhamento de portas;
- 20. Deve implementar 802.1x;
- 21. Deve implementar autenticação baseada em web;
- 22. Deve implementar autenticação baseada em endereço MAC;
- 23. Deve implementar TACACS+. Não serão aceitas soluções similares;
- 24. Deve implementar SNMP;
- 25. Deve suportar duas imagens de software na memória flash;
- 26. Deve suportar múltiplos arquivos de configuração na memória flash;
- 27. Deve implementar sFlow (IPv4 e IPv6);
- 28. Deve possuir interface web para configuração;
- 29. Deve implementar TR-069;
- 30. Deve implementar Syslog;
- 31. Deve implementar nativamente 4 (quatro) grupos RMON (Estatísticas, Históricos, Alarmes e Eventos)
- 32. Deve implementar Secure FTP (SFTP);
- 33. Deve implementar SNMP v1/v2/v3;

34. O equipamento não pode constar na lista de produtos e com anúncio de end-of sales pelo fabricante;
35. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
36. Deve implementar o isolamento de um Access Point rogue conectado ao switch, quando este for detectado por solução de WLAN do mesmo fabricante;
37. 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;
38. Deve possuir interface REST API ;
39. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE”
40. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote);
41. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;

Licenciamento

42. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
43. 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

44. Deve possuir garantia enquanto o produto estiver em linha de fabricação.
45. O fabricante deverá enviar um equipamento novo, em caso de falha do adquirido na modalidade NBD pelo período de 36 meses.
46. Deve permitir suporte por telefone ou website para configurações básicas, apenas.
47. Deve fornecer acesso ao website do fabricante para leitura da documentação do equipamento, em caso de necessidade.

11 SWITCH ACESSO 24 PORTAS POE

10

1. Deve possuir 24 portas 10/100/1000;
2. Deve possuir 4 portas 1 GbE SFP;
3. Deve possuir capacidade de encaminhamento de, no mínimo, 41 Mpps;
4. Deve possuir capacidade de comutação de, no mínimo, 56 Gbps;
5. Deve implementar PoE+ (IEEE 802.3at) em cada porta 10/100/1000BaseT. A fonte interna do switch deve disponibilizar 195w de potência para alimentação do conjunto de portas PoE+;
6. Deve possuir uma interface de console USB;
7. Deve prover endereçamento IP para o gerenciamento de até 16 switches individualmente;
8. Deve suportar agregação de link através de LACP;
9. Deve possuir 16.000 endereços MAC;
10. Deve possuir latência máxima de 3 µs, considerando pacotes de 64 bytes nas interfaces 1 GbE;
11. Deve suportar sflow através da RFC 3176;
12. Deve possuir buffers de, no mínimo, 1.5 MB;

13. Deve implementar 512 VLANs simultaneamente;
 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 MLD snooping;
 19. Deve implementar IGMP v3;
 20. Deve suportar espelhamento de portas;
 21. Deve implementar 802.1x;
 22. Deve implementar autenticação baseada em web;
 23. Deve implementar autenticação baseada em endereço MAC;
 24. Deve implementar TACACS+. Não serão aceitas soluções similares;
 25. Deve implementar SNMP;
 26. Deve suportar duas imagens de software na memória flash;
 27. Deve suportar múltiplos arquivos de configuração na memória flash;
 28. Deve implementar sFlow (IPv4 e IPv6);
 29. Deve possuir interface web para configuração;
 30. Deve implementar TR-069;
 31. Deve implementar Syslog;
 32. Deve implementar nativamente 4 (quatro) grupos RMON (Estatísticas, Históricos, Alarmes e Eventos)
 33. Deve implementar Secure FTP (SFTP);
 34. Deve implementar SNMP v1/v2/v3;
 35. O equipamento não pode constar na lista de produtos e com anúncio de end-of sales pelo fabricante;
 36. Deve possuir interface REST API ;
 37. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE”
 38. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
 39. Deve implementar o isolamento de um Access Point rogue conectado ao switch, quando este for detectado por solução de WLAN do mesmo fabricante;
 40. 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, potência PoE e prioridade PoE;
 41. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote);
 42. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;
- Licenciamento**
43. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;

	<p>44. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;</p> <p>Garantia e Suporte</p> <p>45. Deve possuir garantia enquanto o produto estiver em linha de fabricação.</p> <p>46. Deve permitir suporte por telefone ou website para configurações básicas, apenas.</p> <p>47. Deve fornecer acesso ao website do fabricante para leitura da documentação do equipamento, em caso de necessidade.</p>	
12	<p>TRANSCEIVER 1G SX</p> <p>1. Deve suportar padrão 1000Base-SX com conector do tipo SFP;</p> <p>2. Deve possuir conector LC;</p> <p>3. Suportar distância de até 500m em fibra multimodo;</p> <p>4. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote).</p>	120
13	<p>TRANSCEIVER 10G SR</p> <p>1. Deve suportar padrão 10GBASE-SR com conector do tipo SFP+;</p> <p>2. Deve possuir conector LC;</p> <p>3. Suportar distância de até 300 metros em fibra multimodo;</p> <p>4. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este item, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote).</p>	8

14	<p>SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO</p> <p>1. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da Contratada e/ou fabricante, que deverão possuir capacidade técnica necessária à execução do serviço;</p> <p>2. Os trabalhos deverão ser realizados dentro do horário comercial, das 08:00 às 18:00, salvo casos onde necessite parada no ambiente que demande janelas de manutenção. Neste último caso, deve ser negociado os horários com antecedência;</p> <p>3. Deve ser realizado previamente ao início dos trabalhos uma análise da topologia e arquitetura da rede, considerando os roteadores, switches e demais equipamentos de infraestrutura já existentes;</p> <p>4. Deve realizar as configurações de acordo com as melhores práticas do fabricante;</p> <p>5. Deve ser considerado um pacote de 40 horas de serviço on-site para instalação de configuração. Este serviço poderá incluir:</p> <p>6. Configuração lógica dos Pontos de Acesso, Controladora e software de controle de acesso;</p> <p>7. Instalação física das controladoras WLAN adquiridas no local determinado pela equipe responsável do projeto;</p> <p>8. Criação de Template de configuração;</p> <p>9. Inclusão dos Pontos de Acesso e Controladoras Virtuais no Software de Gerenciamento;</p> <p>10. Parte do pacote de horas poderá ser utilizado a critério do órgão para repasse de informação no formato de treinamento para a equipe da Contratante;</p> <p>11. Deverá entregar documentação detalhada ao final da realização dos trabalhos contendo o passo-a-passo de toda instalação e configuração dos equipamentos envolvidos no projeto.</p>	1
-----------	---	----------

4.1. Requisitos de Capacitação

Deverá ser realizada capacitação do corpo técnico para a administração e gerenciamento do ambiente.

Além de ser uma capacitação para criação, manutenção e administração do ambiente, a capacitação é também considerada como um importante requisito de manutenção já que, após o fim do contrato, é importante que a equipe tenha domínio total para manter a solução em pleno funcionamento.

Em função da equipe já estar familiarizada com produtos de rede já instalados, deverá ser ministrado um treinamento do tipo hand's on com duração de pelo menos 8 (oito) horas pelo técnico responsável pela implementação. Este treinamento deverá estar orientado as tarefas e funcionalidades de administração diárias.

4.2. Requisitos Legais

- a. Lei nº 8.666, de 21 de julho de 1993, que institui normas para licitações e contratos da Administração Pública.
- b. Lei nº 10.520, de 17 de julho de 2002, que institui modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.
- c. Lei nº 8.248, de 23 de outubro de 1991, que dispõe sobre a capacitação e competitividade do setor de informática e automação.
- d. Decreto nº 3.555, de 08 de agosto de 2000, que aprova o regulamento para modalidade de licitação denominado pregão, para aquisição de bens e serviços comuns.
- e. Decreto nº 5.450, de 31 de maio de 2005, que regulamenta o pregão, na forma eletrônica, para bens e serviços comuns.

4.3. Requisitos de Manutenção

A garantia técnica da Solução deverá ser prestada conforme especificado dentro de cada item descrito no termo de referência deste documento.

Os técnicos envolvidos deverão estar treinados no processo de instalação e configuração do ambiente. Recomendável manter o contrato de suporte com o fabricante vigente, a fim de minimizar riscos em caso de falhas de software/hardware (se houver) e bugs de sistema. Dentre as vantagens de possuir um contrato de manutenção ativo, destacam-se:

- a. Hardware: possibilidade de troca de equipamento ou peça no caso de falha, possibilidade de atualização de firmware para

melhoria de operação ou utilização de novos recursos do equipamento, suporte do fabricante na resolução de problemas graves.

b. Software: possibilidade de atualização das versões de software durante o período de garantia. As atualizações são úteis para resolução de problemas (bugs), correções de segurança e implantação de novos recursos/funcionalidades da solução.

A Contratada ou fabricante deverá disponibilizar “Central de Atendimento” para abertura de chamado, em dias úteis, (segunda-feira a sexta-feira), indicando telefone do tipo 0800 ou através de e-mail.

4.4. Requisitos Temporais

Deverá ser realizada após a assinatura do Contrato, uma reunião de alinhamento remota, com o objetivo de alinhar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e em seus Anexos, e esclarecer possíveis dúvidas acerca do objeto, conforme agendamento efetuado pelo Gestor do Contrato, bem como:

- a. Apresentar a relação do pessoal técnico especializado, adequado e disponível para a execução do objeto deste Estudo, bem como a qualificação de cada um dos membros da equipe técnica.
- b. Apresentar a declaração de disponibilidade, assinada por cada integrante da equipe técnica mencionada na alínea anterior, bem como o Termo de Confidencialidade da Informação.
- c. Apresentar um cronograma para implantação e configuração da Solução adquirida, o qual deverá sofrer aval do Gestor do Contrato.
- d. Apresentar a logística para realização do treinamento oficial do fabricante da Solução adquirida.

Os profissionais indicados pela Contratada deverão efetivamente implantar e configurar a Solução, objeto deste Estudo, admitindo-se suas substituições por profissionais de experiência equivalente ou superior, desde que aprovadas previamente pelo IFPI.

O prazo para a entrega, instalação e configuração da solução será de até 120 (cento e vinte) dias consecutivos, contados a partir do primeiro dia útil após a data da última assinatura do Contrato.

4.5. Requisitos de Segurança

- a. Fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução dos serviços de instalação da Solução;

4.6. Requisitos Sociais, Ambientais e Culturais

- a. Usar equipamentos, quando aplicável, homologados pela Anatel e/ou ABNT, no que diz respeito a normas ambientais;
- b. Usar produtos de limpeza e conservação de superfícies e objetos inanimados que obedeçam às classificações e especificações determinadas pela ANVISA;
- c. Respeitar as Normas Brasileiras - NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos, incluindo práticas de logística reversa, conforme o caso;
- d. Dar preferência ao uso de bens constituídos por material reciclado, atóxico, biodegradável, conforme ABNT NBR - 15448-1 e 15448-2;
- e. Acondicionar os bens preferencialmente em embalagem individual adequada, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;
- f. Que os bens não contenham substâncias perigosas em concentração acima das recomendadas pelas normas técnicas;
- g. Todos documentos ou artefatos gerados pela contratada, salvo manifestação explícita pelo IFPI deverão ser entregues em formato digital; e
- h. A documentação dos produtos que integram a presente solução deverá estar, preferencialmente, na língua portuguesa do Brasil.

4.7. Requisitos de Arquitetura Tecnológica

- a. Disponibilidade de espaço físico nos racks do datacenter para instalação de hardwares disponíveis. E no datacenter, espaço lógico disponível para criação de ambiente virtualizado para instalação dos softwares contidos nas soluções apresentadas neste documento.

4.8. Requisitos de Projeto e de Implantação

- a. Disponibilidade de espaço físico nos racks onde as controladoras serão instaladas;
- b. Infraestrutura elétrica e de rede ethernet para a instalação dos pontos de acesso;
- c. Alimentação elétrica para os equipamentos;

d. Servidores com capacidade disponíveis para criação de ambiente virtualizado para instalações das soluções apresentadas neste documento;

4.9. Requisitos de Garantia

O mercado de ativos de dados sem fio, assim como qualquer mercado de equipamentos eletrônicos, é inundado de equipamentos de baixíssima qualidade que, embora possam ter um custo inicial menor, sem dúvidas têm um custo superior ao longo do tempo por conta da demanda frequente por manutenção. Outrossim, há de se afastar a possibilidade de que o equipamento de rede falhe precisamente quando seja necessário.

Desta forma, se faz necessária uma especificação que determine um critério mínimo de qualidade aceitável para os equipamentos mais críticos ao sistema.

Os serviços de garantia deverão ser prestados pelo próprio fabricante da solução ofertada ou por empresa autorizada oficialmente pelo fabricante para prestar este tipo de serviço no Brasil.

O prazo de garantia/suporte mínima deverá ser de 36 (trinta e seis) meses, para todos os equipamentos/licenças, contado a partir da data do ACEITE DEFINITIVO, exceto quando estiver especificado nas características individuais de cada objeto no termo de referência.

4.10. Requisitos de Experiência Profissional

A implantação deve ser realizada por profissionais especializados da contratada e/ou próprio fabricante para a solução proposta, que possuam certificações na tecnologia da solução adquirida, rede de dados sem fio, que lhes confirmam as competências necessárias para a realização dos respectivos serviços.

4.11. Requisitos de Formação da Equipe

PERFIL - ESPECIALISTA NA SOLUÇÃO DE REDE DE DADOS	
Responsável por realizar todas as atividades relacionadas à implementação e testes da solução de rede cabeada e rede, conforme as normas, padrões e diretrizes da contratante, implementando os casos de uso, integrando os componentes propostos com os existentes, além de gerar e manter as rotinas de implantação.	
Experiência/Qualificação	Modo de Comprovação
Experiência mínima de 04 (quatro) anos em implementação em rede de dados	Registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.
Formação	Modo de Comprovação
Curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação.	Diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou mestrado ou doutorado, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.

4.12. Requisitos de Segurança da Informação

a) A empresa fornecedora da Solução é integralmente responsável pela manutenção de sigilo sobre quaisquer dados e informações fornecidos pelo IFPI ou contidos em quaisquer documentos e em quaisquer mídias de que venham a ter conhecimento durante a etapa de repasse, de execução dos trabalhos e de encerramento dos serviços, não podendo, se não formalmente autorizado pelo IFPI, sob qualquer pretexto e forma, divulgá-los, reproduzi-los ou utilizá-los a qualquer tempo;

b) A empresa deverá possuir nas suas instalações, onde atividades serão executadas de modo remoto, padrões de segurança da informação e de tecnologia da informação para evitar a perda ou o vazamento, ataques externos e tentativas de invasão, como firewall e sistemas antivírus;

c) Cada profissional a serviço da empresa deverá assinar o Termo de Sigilo e Responsabilidade da Política de Segurança de TIC do IFPI, bem como declaração de estar ciente de que a estrutura computacional do IFPI não poderá ser utilizada para fins diversos daqueles do objeto relacionado à prestação do serviço;

d) O correio eletrônico e a navegação em sítios da internet a partir do ambiente de rede do IFPI poderão, a exclusivo critério do IFPI, ser objeto de controle e auditoria;

e) Quando se contrata uma Solução de Tecnologia da Informação e Comunicação (STIC) em sua integralidade, compreendendo todas as fases de sua execução, serviços e instalações necessárias, sob a responsabilidade da empresa contratada até sua definitiva entrega do objeto pretendido ao contratado, é de bom alvitre que sejam verificados, com a acuracidade necessária, todos os requisitos de segurança da informação e comunicação mitigando sobremaneira a vulnerabilidade ameaçadora da integridade e privacidade corporativa, potencialmente existente;

f) A Contratada deverá configurar de maneira apropriada os elementos de rede para habilitar o log dos eventos da rede do IFPI, tais como conexões externas e registros de utilização de serviços (arquivos transferidos via FTP, acessos a páginas web e tentativas de login não autorizado);

g) Os logs devem estar com o horário sincronizado via NTP e possuir o quanto possível de detalhes, sem, no entanto, gerar dados em excesso. A Contratada deverá configurar os elementos da rede para enviar os logs para um Servidor de Logs dedicado, disponibilizado pelo IFPI;

h) A Contratada deverá aplicar e manter atualizados os patches de segurança nos equipamentos que compõem a Solução; e

i) Os ativos de rede deverão suportar autenticação 802.1x, listas de controle de acesso (ACLs) e proteção por usuário e senha de todas as ferramentas de gerenciamento, tais como: web, SSH e console.

5 – RESPONSABILIDADES

5.1. Requisitos de Capacitação

- a) Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- b) Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico;
- c) Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- d) Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
- e) Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- f) Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- g) Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável; e
- h) Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração.

5.2. Deveres e responsabilidades da CONTRATADA

- a) Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato;
- b) Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- c) Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;
- d) Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;
- e) Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- f) Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- g) Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e
- h) Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração.

5.3. Deveres e responsabilidades do órgão gerenciador da ata de registro de preços

- a) Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;
- b) Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;
- c) Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:
 - 1) as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e
 - 2) definição dos eventos a serem reportados ao órgão gerenciador, com indicação de prazo e responsável.
- d) Definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:
 - 1) a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;
 - 2) as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pela contratada; e
 - 3) as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a realização de Prova de Conceito, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

6 – MODELO DE EXECUÇÃO DO CONTRATO

6.1. Quantidade mínima de bens ou serviços para comparação e controle

Lote	Id.	Descrição	Quantidade
1	1	PONTO DE ACESSO INTERNO	125
	2	CONTROLADORA DOS PONTOS DE ACESSO	2
	3	LICENÇAS DE PONTOS DE ACESSO PARA CONTROLADORA	125
	4	INJETOR POE+	125
	5	SISTEMA DE GERENCIAMENTO	1
	6	LICENÇA PARA SOFTWARE DE GERENCIAMENTO	248
	7	SWITCH DISTRIBUIÇÃO	8
	8	SWITCH ACESSO 48 PORTAS	30
	9	SWITCH ACESSO 48 PORTAS POE	10
	10	SWITCH ACESSO 24 PORTAS	70
	11	SWITCH ACESSO 24 PORTAS POE	10
	12	TRANSCEIVER 1G SX	120
	13	TRANSCEIVER 10G SR	8
	14	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO	1

6.2. Manutenção de Sigilo e Normas de Segurança

A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

7 – MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de Aceitação

Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos remanufaturados, NFR (Not For Resale) ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas.

O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente nas especificações técnicas deste termo de referência.

Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital.

8 – ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

Lote	Id.	Descrição	Quantidade	UN	Valor Unitário Máximo	Valor Total Máximo
1	1	PONTO DE ACESSO INTERNO	125	UN	R\$ 6.491,45	R\$ 811.431,67
	2	CONTROLADORA DOS PONTOS DE ACESSO	2	UN	R\$ 196.637,46	R\$ 393.274,92
	3	LICENÇAS DE PONTOS DE ACESSO PARA CONTROLADORA	125	UN	R\$ 2.849,27	R\$ 356.158,33
	4	INJETOR POE+	125	UN	R\$ 1.235,38	R\$ 154.422,50
	5	SISTEMA DE GERENCIAMENTO	1	UN	R\$ 982,78	R\$ 982,78
	6	LICENÇA PARA SOFTWARE DE GERENCIAMENTO	248	UN	R\$ 982,78	R\$ 243.729,44
	7	SWITCH DISTRIBUIÇÃO	8	UN	R\$ 113.114,52	R\$ 904.916,13
	8	SWITCH ACESSO 48 PORTAS	30	UN	R\$ 18.649,12	R\$ 559.473,60
	9	SWITCH ACESSO 48 PORTAS POE	10	UN	R\$ 31.315,44	R\$ 313.154,37
	10	SWITCH ACESSO 24 PORTAS	70	UN	R\$ 10.481,98	R\$ 733.738,60
	11	SWITCH ACESSO 24 PORTAS POE	10	UN	R\$ 18.071,80	R\$ 180.718,00
	12	TRANSCEIVER 1G SX	120	UN	R\$ 1.789,37	R\$ 214.724,80
	13	TRANSCEIVER 10G SR	8	UN	R\$ 6.555,02	R\$ 52.440,16
	14	SERVIÇO DE INSTALAÇÃO E REPASSE DE CONHECIMENTO	1	UN	R\$ 38.538,80	R\$ 38.538,80

9 – DA VIGÊNCIA DO CONTRATO

O contrato vigorará por 12 (doze) meses, contados a partir da data da sua assinatura, podendo ser prorrogado por períodos iguais e sucessivos, limitado a 24 (vinte e quatro) meses, desde que haja preços e condições mais vantajosas para a Administração, nos termos do Inciso II, Art. 57, da Lei nº 8.666, de 1993.

A prorrogação do contrato dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada de a realização de pesquisa de mercado que demonstre a vantajosidade dos preços contratados para a Administração.

10 – DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. Critérios de Qualificação Técnica para a Habilitação

Efetuada a verificação referente ao cumprimento das condições de participação no certame, a habilitação das licitantes será realizada mediante a apresentação da seguinte documentação complementar:

- a. Atestado de Capacidade Técnica demonstrando que a proponente forneceu equipamentos, para pessoa física ou jurídica de direito público ou privado, e realizou a instalação de soluções compatíveis com os objetos deste termo de referência;
- b. O atestado acima referido deverá conter identificação do emitente, características e localização da prestação do serviço, local, data da expedição e declaração do emitente de que o serviço foi realizado a contento.
- c. A contratada deverá possuir, pelo menos, 01 (um) técnico certificado oficial na solução de rede sem fio, apresentado neste termo de referência;
1. A comprovação de vínculo profissional se fará com a apresentação de cópia da carteira de trabalho (CTPS) em que conste o licitante como contratante; do contrato social do licitante em que conste o profissional como sócio; do contrato de prestação de serviços, sem vínculo trabalhista, regido pela legislação civil ou, ainda, de declaração de contratação futura do profissional, desde que acompanhada de declaração de anuência do profissional.
- d. Apresentar declaração do fabricante comprovando que os itens ofertados possuem garantia no Brasil.
- e. Comprovar pertencer ao ramo de atividade pertinente aos objetos da contratação, através de cartão CNPJ, estatuto ou contrato social em vigor devidamente registrado na Junta Comercial.

E com a finalidade de garantir que a licitante será capaz de fornecer os equipamentos, prestar os serviços envolvidos e a garantia técnica, bem como garantir a originalidade de todos os equipamentos, sua participação no certame está condicionada à comprovação de capacidade técnica. Assim, a licitante deverá:

- a. Comprovar aptidão do desempenho de atividade pertinente e compatível em tecnologia com a solução global especificada neste Termo de Referência. A comprovação deverá acontecer através da apresentação de declaração dos fabricantes dos equipamentos e softwares, garantindo que a proponente é capaz de fornecer, instalar, configurar e prestar suporte da solução ofertada, não implicando em perda de garantia no Brasil.

11 – JUSTIFICATIVA PARA ADOÇÃO DO SRP

A saber, o decreto 7.892/2013 prevê em seu artigo 3º o seguinte:

Art. 3º O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:

- I. quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;
- II. quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;
- III. quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; ou
- IV. quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

Para a criação de novas salas, reestruturação da rede lógica dos campi e expansão dos recursos computacionais existentes, é necessária a implantação de novos equipamentos de rede LAN e WIFI, porém não é possível afirmar com o mínimo de precisão qual será a demanda exata resultante dessas novas cargas de trabalho.

Além disso, temos a evolução constante das demandas que motivam esse projeto (implantação de projetos, pesquisas e demandas recorrentes de setores de todo o IFPI, sistemas existentes e demandas futuras do Processo Eletrônico Nacional e SUAPEDU) ocorre seguindo uma dinâmica não-linear e pouco previsível.

Outro ponto é quanto ao orçamento para aquisição da solução, o IFPI atualmente não possui orçamento próprio para esta demanda, porém o orçamento poderá vir a ser adquirido através de termo de execução descentralizada - TED.

Ante ao exposto, fica evidente que a contratação se enquadra no inciso IV do referido decreto, visto que não é possível definir previamente o quantitativo a ser demandado pela Administração.

12 – JUSTIFICATIVA PARA NÃO APLICAÇÃO DA RESERVA DE COTA

A saber, a Lei Complementar Federal nº 123, de 14/12/2006 dispõe, no Art. 48, que licitações com valores estimados superiores a R\$ 80.000,00 (Oitenta mil reais), deverá a administração “[...] estabelecer, em certames para aquisição de bens de natureza divisível, cota de até 25% (vinte e cinco por cento) do objeto para a contratação de microempresas e empresas de pequeno porte”, exceto quanto ocorrer alguma das situações previstas no art. 49 como exceções: quando “não houver um mínimo de 3 (três) fornecedores competitivos enquadrados como microempresas ou empresas de pequeno porte sediados local ou regionalmente e capazes de cumprir as exigências estabelecidas no instrumento convocatório” ou quando “o tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte não for vantajoso para a administração pública ou representar prejuízo ao conjunto ou complexo do objeto a ser contratado” (grifos nossos).

Primeiramente é preciso considerar a impossibilidade de divisão dos itens que compõe o certame, pois os equipamentos, sistemas e serviços que constituem a solução interagem entre si de forma a convergir para um sistema unificado, de modo que o fornecimento parcelado inviabilizaria a implantação de tecnologia capaz de atender as necessidades deste órgão. A eventual divisão do objeto em grupos diversos poderia ocasionar situações de fornecimento de equipamentos e/ou softwares incompatíveis entre si.

Ante ao exposto, é evidente que o agrupamento do objeto, de maneira a compor uma solução unificada, é necessário a fim de evitar eventuais problemas de compatibilidade.

Ademais, lidar com um único fornecedor diminui o custo administrativo de gerenciamento de todo o processo de contratação. O aumento da eficiência administrativa do setor público passa pela otimização do gerenciamento de seus contratos de fornecimento. Essa eficiência administrativa também é de estatura constitucional e deve ser buscada pela administração pública.

Outrossim, o agrupamento em lote de todos os equipamentos visa garantir a otimização dos prazos de execução, viabilizando a sincronia nos fornecimentos e instalações visto a complexidade do projeto, evitando assim que um fornecedor venha a prejudicar a execução de outro.

Salienta-se ainda que não há no estado do Piauí empresas capazes de cumprir as exigências do instrumento convocatório, enquadrando-se, portanto, na primeira condição de exceção prevista em lei.

A segunda condição de exceção prevista em lei também é presente, posto que o agrupamento resultante da não divisão do objeto produz a redução dos preços. Uma disposição em contrário poderia colocar em risco a economia de escala e a celeridade processual, comprometendo a seleção da proposta mais vantajosa para a administração.

13 – ESTRATÉGIAS PARA EVITAR JOGO DE PLANILHAS

O jogo de planilhas consiste na atribuição de preços significativamente menores a itens que terão seus quantitativos reduzidos ou que não serão executados, e de valores elevados a itens cuja estimativa é inferior à que será efetivamente demandada na execução, “autorizando” o contratado a solicitar reajuste contratual cujo deferimento implica aumento substancial do valor da proposta (CAMPITELI, 2006).

A principal estratégia para se evitar o jogo de planilhas é o estabelecimento de critérios de aceitabilidade dos preços unitários e global, conforme pregado na ORIENTAÇÃO NORMATIVA Nº 5, DE 1º DE ABRIL DE 2009 da AGU. Com base nisso, é conclusivo que, embora a contratação ocorra por melhor preço global, devem ser definidos preços unitários cujos critérios de aceitabilidade estabeleçam como valores-teto os preços médios de mercado.

Assim sendo, uma vez delineado o escopo e os requisitos técnicos mínimos para os equipamentos que comporão a solução, detalhados no estudo técnico preliminar da contratação, o setor de tecnologia da informação realizou extensa busca no SIASG a procura de atas de registro de preços válidas e com equipamentos compatíveis às especificações do termo de referência confeccionado a fim de obter uma referência de preços precisa. O resultado desta busca é listado abaixo:

- Ata nº1 – MINISTERIO DA DEFESA – PREGAO 118/CAE/2020 SRP - PROCESSO ADMINISTRATIVO 67106.000113/2020-50
- Ata nº2 - COMANDO DA AERONAUTICA – PREGAO 121/GAP-SJ/2019 PROCESSO ADMINISTRATIVO 67720.019430/2018-88
- Ata nº 3 - UFPI – PREGAO 47/2018 – PROCESSO ADMINISTRATIVO 23111.043923/2018-70

Importante observar que houve grande variação da cotação do dólar desde a data provável de tomada de preços das ARP supracitadas, assim, com o mesmo propósito de estipular o preço de referência mais preciso, foi feita a correção dos preços segundo variação do dólar e IPCA do período:

- <https://www.bcb.gov.br/estabilidadefinanceira/historicocotacoes>
- <https://www3.bcb.gov.br/CALCIDADAOPublico/exibirFormCorrecaoValores.do?method=exibirFormCorrecaoValores>

Nesse mesmo sentido, a fim de validar os preços calculados, também foi realizada consulta à potenciais fornecedores:

- Fornecedor 1 – CLM Software Comércio, Importação e Exportação Ltda.
- Fornecedor 2 – TECNO-IT Tecnologia e Serviços LTDA
- Fornecedor 3 - APPROACH TECNOLOGIA

Por fim, considerando que a caracterização do jogo de planilhas independe da demonstração de dolo das partes envolvidas, a elaboração de projeto básico suficientemente detalhado a fim de garantir uma compreensão perfeita e igual entre os licitantes é estratégia complementar para evitar a ocorrência não dolosa dessa prática.

14 – DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 1432/2020, de 19 de agosto de 2020.

Conforme o §6º do art. 12 da IN SGD/ME nº 01, de 2019, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

_____ Integrante Requisitante Paulo Alex dos Santos Maranhão Analista de Tecnologia da Informação Matrícula/SIAPE: 1263948	_____ Integrante Técnico Benedito Enaldo Araújo de Oliveira Técnico de Tecnologia da Informação Matrícula/SIAPE: 2291407	_____ Integrante Administrativo Leonardo de Macedo Carvalho Assistente em Administração Matrícula/SIAPE: 1808241
---	---	---

Autoridade Máxima da Área de TIC

Eduilson Lívio Neves da Costa Carneiro
Matrícula/SIAPE: 1287949
Teresina, 01 de Dezembro de 2020

Aprovo,

Autoridade Competente

Paulo Borges da Cunha
Matrícula/SIAPE: 1288003
Teresina, 01 de Dezembro de 2020

Teresina/PI, 01 de Dezembro de 2020

Documento assinado eletronicamente por:

- **Leonardo de Macedo Carvalho**, ASSISTENTE EM ADMINISTRACAO , em 10/12/2020 10:17:47.
- **Eduilson Livio Neves da Costa Carneiro**, DIRETOR - CD3 - DTI-IFPI, em 07/12/2020 10:12:05.
- **Paulo Borges da Cunha**, PRO-REITOR - CD2 - PROAD-IFPI, em 03/12/2020 09:35:09.
- **Paulo Alex dos Santos Maranhao**, CHEFE DE DEPARTAMENTO - CD4 - DRT-IFPI, em 03/12/2020 09:05:56.
- **Benedito Enaldo Araujo de Oliveira**, TEC DE TECNOLOGIA DA INFORMACAO , em 02/12/2020 18:49:12.

Este documento foi emitido pelo SUAP em 01/12/2020. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifpi.edu.br/autenticar-documento/> e forneça os dados abaixo:

Código Verificador: 13966

Código de Autenticação: 2e4d14aaa9

