Serviço Público Federal
Conselho Federal de Medicina Veterinária

INFORMAÇÃO 5/2025 - GETIC/SUPEX/DE/CFMV/SISTEMA

Em 30 de janeiro de 2025.

Ao Senhor
Pregoeiro do CFMV
Vitor Hugo da Silva Ramos

Assunto**: Resposta à SOLICITAÇÃO 4/2025 - SELIC/GERAD/SUPEX/DE**

Senhor Pregoeiro,

1. Em resposta ao seu pedido de manifestação técnica enviado ao Setor de Infraestrutura e Segurança da Informação - SESEG/GETIC, referente à qualificação técnica da licitante e demais documentos necessários, conforme os requisitos exigidos no **Pregão Eletrônico nº 90012/2024**, do PA nº **0110044.00000049/2024-74**; informamos que foi analisada a documentação da empresa **BSB TIC SOLUÇÕES LTDA.**

2. Foram analisados os documentos enviados pela licitante em relação às Especificações Técnicas, Habilitação e Qualificação Técnica, quanto ao atendimento das condições previstas no edital, em especial, a:

2.1. QUALIFICAÇÃO TÉCNICA;

2.2. PROPOSTA COMERCIAL;

3. Identificou-se o seguinte:

a) A empresa licitante apresentou proposta **compatível** com as especificações do edital;

b) A empresa apresentou **27 (vinte e sete) atestados** de capacidade técnica, dos quais **apenas um é compatível** com o objeto da licitação. Isso comprova o fornecimento de pontos de acesso no total de 50% (cinquenta) do montante solicitado neste certame, conforme item 9.31 do TR;

c) Foi realizada uma diligência com a licitante para obter informações detalhadas sobre a solução proposta. A empresa enviou o ANEXO G preenchido e, posteriormente, complementou a informação por e-mail. Diante o exposto, constatou-se que todas as funcionalidades da solução apresentada atendem às especificações do edital.

4**. DECISÃO**: Portanto, a empresa BSB TIC SOLUÇÕES LTDA **atende** aos requisitos do edital.

Atenciosamente,

Marcia Fernanda de Macedo Marto
Analista de Rede do Setor de Infraestrutura - SESEG
Gerência de Tecnologia da Informação e Comunicação - GETIC
Matr. CFMV nº 0652

Documento assinado eletronicamente por:

- **Márcia Fernanda de Macedo Marto**, **Empregado - CMSUP - SESEG**, em 30/01/2025 16:53:05.
- **Lincoln Máximo Alves, Chefe do Setor - FGSUP - SEINF**, em 30/01/2025 17:03:02.

Este documento foi emitido pelo SUAP em 30/01/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.cfmv.gov.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 401243
Código de Autenticação: e76b03b48e

Marcia Fernanda de Macedo Marto

De: Informática GETIC-CFMV
Enviado em: quinta-feira, 30 de janeiro de 2025 16:29
Para: 'Bsb Tecnologia'; Informática GETIC-CFMV
Cc: diretoria@bsbtecnologia.com.br; Luciana Alves
Assunto: RES: RES: Anexo G – Tabela de cumprimento dos Requisitos

Boa tarde Luciana.

Recebemos a planilha atualizada.

At.te

Marcia Fernanda de Macedo Marto
Setor de Infraestrutura e segurança da Informação - SESEG
Conselho Federal de Medicina Veterinária
(61) 2106-0457

De: Bsb Tecnologia <financ.bsb@gmail.com>
Enviada em: quinta-feira, 30 de janeiro de 2025 16:18
Para: Informática GETIC-CFMV <informatica@cfmv.gov.br>
Assunto: Re: RES: Anexo G – Tabela de cumprimento dos Requisitos

Boa tarde Márcia,
Segue anexo palnilha corrigida.
Att,

Em qui., 30 de jan. de 2025 às 15:11, Informática GETIC-CFMV <informatica@cfmv.gov.br> escreveu:

> Boa tarde Luciana.
>
> Confirme o recebimento do email e se sua solução atende aos requisitos.
>
> At.te

Marcia Fernanda de Macedo Marto
Setor de Infraestrutura e segurança da Informação - SESEG
Conselho Federal de Medicina Veterinária
(61) 2106-0457

De: Informática GETIC-CFMV <informatica@cfmv.gov.br>
Enviada em: quinta-feira, 30 de janeiro de 2025 10:13
Para: Luciana Alves <admbsbtecnologia@gmail.com>
Cc: diretoria@bsbtecnologia.com.br; Informática GETIC-CFMV <informatica@cfmv.gov.br>
Assunto: RES: RES: Anexo G – Tabela de cumprimento dos Requisitos

Bom dia Luciana.

Informo que no Anexo G enviado faltaram as informações abaixo.

Fizemos uma pesquisa na internet e encontramos o recurso denominado **cnMaestro X Assurance** da Cambium Networks, que utiliza tecnologia de inteligência artificial e machine learning. Gostaríamos de saber se a proposta contempla este recurso e se ele será entregue.

DESCRIÇÃO DOS REQUISITOS MÍNIMOS PARA CONTROLADORA WIRELESS VIRTUAL	DOCUMENTO/PÁGINA

5	**CARACTERÍSTICAS GERAIS**	
5.15	Balancear automaticamente a carga de usuários através de múltiplos pontos de acesso.	
5.16	Deverá implementar mecanismos de inteligência artificial para operações de TI (AIOPS).	
5.17	Deverá utilizar a tecnologia AI (inteligência artificial) e ML (Machine Learning) para interpretar eventos e fornecer insights com recomendações para resolução de problemas.	
5.18	Possuir capacidade de geração de relatórios ao menos dos seguintes tipos: i) lista dos clientes wireless; ii) lista dos APs; iii) informações de configuração WLAN; iv) utilização da rede.	
5.19	A solução deverá possuir gerenciamento centralizado com emissão de relatórios e estatísticas com **histórico** de utilização de **pelo menos 30 (trinta) dias**.	
5.20	Deverá ser do mesmo fabricante dos pontos de acesso do ITEM 1 para fins de total compatibilidade e gerenciamento unificado da solução.	

Aguardo retorno.

At.te

Marcia Fernanda de Macedo Marto
Setor de Infraestrutura e segurança da Informação - SESEG
Conselho Federal de Medicina Veterinária
(61) 2106-0457

De: Informática GETIC-CFMV <informatica@cfmv.gov.br>
Enviada em: quarta-feira, 29 de janeiro de 2025 15:04
Para: Luciana Alves <admbsbtecnologia@gmail.com>; Informática GETIC-CFMV <informatica@cfmv.gov.br>
Assunto: RES: RES: Anexo G – Tabela de cumprimento dos Requisitos

Luciana,

Planilha recebida.

At.te

Marcia Fernanda de Macedo Marto
Setor de Infraestrutura e segurança da Informação - SESEG
Conselho Federal de Medicina Veterinária
(61) 2106-0457

De: Luciana Alves <admbsbtecnologia@gmail.com>
Enviada em: quarta-feira, 29 de janeiro de 2025 15:02
Para: Informática GETIC-CFMV <informatica@cfmv.gov.br>
Assunto: Re: RES: Anexo G – Tabela de cumprimento dos Requisitos

Prezada Márcia,

Segue anexo, planilha ponto a ponto.

Att,

Luciana Alves

Analista em Licitações

BSB TIC SOLUÇÕES

Em qua., 29 de jan. de 2025 às 14:14, Informática GETIC-CFMV <informatica@cfmv.gov.br> escreveu:

Luciana,

Prazo concedido.

At.te

Marcia Fernanda de Macedo Marto
Setor de Infraestrutura e segurança da Informação - SESEG
Conselho Federal de Medicina Veterinária
(61) 2106-0457

De: Luciana Alves <admbsbtecnologia@gmail.com>
Enviada em: quarta-feira, 29 de janeiro de 2025 14:09
Para: Informática GETIC-CFMV <informatica@cfmv.gov.br>
Assunto: Re: RES: Anexo G – Tabela de cumprimento dos Requisitos

Prezada Marcia,

Através deste, solicitamos que seja estendido o prazo até as 17horas.

Att,

Luciana Alves

BSB TIC SOLUÇÕES

Em qua., 29 de jan. de 2025 às 09:49, sergio s taveira <sergio@apis.com.br> escreveu:

-------- Mensagem encaminhada --------

Assunto:RES: Anexo G – Tabela de cumprimento dos Requisitos
Data: Tue, 28 Jan 2025 19:26:08 +0000
De: Informática GETIC-CFMV <informatica@cfmv.gov.br>
Para:diretoria@bsbtecnologia.com.br <diretoria@bsbtecnologia.com.br>
CC: Informática GETIC-CFMV <informatica@cfmv.gov.br>

Segue anexo o arquivo.

At.te

Marcia Fernanda de Macedo Marto
Setor de Infraestrutura e segurança da Informação - SESEG
Conselho Federal de Medicina Veterinária
(61) 2106-0457

De: Informática GETIC-CFMV <informatica@cfmv.gov.br>
Enviada em: terça-feira, 28 de janeiro de 2025 16:19
Para: diretoria@bsbtecnologia.com.br
Cc: Informática GETIC-CFMV <informatica@cfmv.gov.br>
Assunto: Anexo G – Tabela de cumprimento dos Requisitos

Prezado senhor Fabrício Chaves,

No Termo de Referência do edital, consta que a empresa deve apresentar um documento apontando o atendimento dos requisitos técnicos da solução (itens 9.44 e 9.48 do TR).

Solicito envio do documento preenchido até **29/1/2025 às 13h** para que possamos dar prosseguimento à habilitação de sua empresa.

Cito:

***Item 9.44**: A LICITANTE dever· apresentar juntamente com a proposta técnica, um documento de Ponto a Ponto para comprovar atendimento dos requisitos técnicos da solução, conforme modelo do **Anexo G – Tabela de cumprimento dos Requisitos**. Sendo esse requisito, motivo de desclassificação, caso não apresentado o documento de ponto a pontos.*

***Item 9.48**: Além de todos os documentos que comprovem os requisitos, deve-se fazer acompanhar a proposta o **ANEXO G - TABELA DE CUMPRIMENTO DE REQUISITOS**, preenchido com a identificação e página do documento onde se encontra descrito cada um dos requisitos da solução.*

At.te

Marcia Fernanda de Macedo Marto
Setor de Infraestrutura e segurança da Informação - SESEG
Conselho Federal de Medicina Veterinária
(61) 2106-0457

.

.

.

This email was scanned by Bitdefender

.

This email was scanned by Bitdefender

Documento Digitalizado Público

Troca de emails com a empresa BSB TIC

Assunto: Troca de emails com a empresa BSB TIC
Assinado por: Marcia Marto
Tipo do Documento: EMAIL
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Documento Original

Documento assinado eletronicamente por:

- **Márcia Fernanda de Macedo Marto**, **Empregado - CMSUP - SESEG**, em 30/01/2025 16:45:47.

Este documento foi armazenado no SUAP em 30/01/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.cfmv.gov.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 976732
Código de Autenticação: f3c2264b21

	DESCRIÇÃO DOS REQUISITOS MÍNIMOS PARA OS PONTOS DE ACESSO	Documento	Pagina
1.1	Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para os produtos conforme resolução nº 715. Não serão aceitos	Cert Anatel	1
1.2	Equipamentos devem ser novos e de primeiro uso.	ok	ok
1.3	Devem ser do mesmo fabricante para fins de total compatibilidade e gerenciamento unificado da solução.	ok	ok
1.4	Devem ser capazes de operar com resiliência e desempenho de modo a permitir alta disponibilidade.	ok	ok
1.5	Devem suportar o gerenciamento centralizado por controlador wireless e possuir funcionalidades de controle abarcadas nos próprios (Access Point) APs permitindo que o gerenciamento e serviços da rede s	ok	ok
1.6	Devem ser acompanhados de todos os acessórios necessários para operacionalização da solução, tais como softwares, documentações técnicas e manuais que contenham informações suficientes, que possibilit	Data AP	3
1.7	Deverá ser fornecido com a versão mais recente do software.	ok	ok
1.8	Possibilitar alimentação elétrica local e via padrão PoE+ (IEEE 802.3at).	Data AP	7
1.9	Possuir, no mínimo, 1 (um) LED para a indicação do status de operação do equipamento	Data AP	2
	2 GERENCIAMENTO DOS APS DOCUMENTO/ PÁGINA		
2.1	Permitir a configuração e gerenciamento direto por meio de browser padrão (HTTPS) e/ou através de plataformas de software que sigam padrões SSH.	Data AP	3
2.2	Caso a solução necessite de controladora, permitir que sua configuração seja realizada automaticamente quando este for conectado.		
2.3	Caso a solução necessite de controladora, permitir que o processo de atualização de software seja realizado manualmente através de interface web, FTP ou TFTP e automaticamente através de controlador W	cnmaestro	182
2.4	Caso a solução necessite de controladora, em caso de falha de comunicação entre os Pontos de Acesso e o controlador WLAN os usuários associados à rede sem fio devem continuar conectados com acesso à r	Data AP	3
2.5	Se um controlador WLAN falhar, os Pontos de Acesso relacionados deverão se associar automaticamente a um controlador WLAN alternativo, não permitindo que a rede wireless se torne inoperante.	Data AP	3
2.6	Implementar mecanismo de funcionamento para trabalhar com controladores WLAN em redundância.	user guide	72
2.7	Implementar funcionamento em modo autogerenciado, sem necessidade de controladora WLAN para configuração de seus parâmetros de rede wireless, gerenciamento das políticas de segurança, QoS e monitorame	user guide	72
2.8	A solução em modo autogerenciado deverá ser redundante e não deverá depender única e exclusivamente de um elemento, ou seja, em caso de falha de um ou mais pontos de acesso a solução deverá continuar	user guide	72
2.9	Deverá permitir a formação de conjuntos de pontos de acesso que se comuniquem e compartilhem das mesmas configurações (Clusters ou Grupos).	user guide	93

2.10	Deverá permitir as seguintes opções de configuração e monitoração: por controlador virtual ou sem o controlador através das funcionalidades de controle embarcadas nos próprios APs.	Data AP	1
2.11	Deverá permitir upgrade de firmware de forma centralizada por um ponto central de gerenciamento.	user guide	182 / 183
2.12	No cenário sem controlador WLAN, o gerenciamento deverá ser centralizado no "AP Mestre", que distribui as configurações de controle para os outros APs da rede.	user guide	61
2.13	Permitir a configuração de um número máximo de clientes que poderão se conectar a um ponto de acesso.	user guide	63
2.14	Quando um ponto de acesso estiver sobrecarregado com muitos usuários deverá permitir o balanceamento destes com outros pontos de acesso.	user guide	69 / 70
2.15	Deverá disponibilizar uma interface gráfica única e centralizada, acessível por browser padrão em página https, para configuração do conjunto de Pontos de Acesso (cluster)	user guide	271
2.16	Deverá suportar a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso no modo autogerenciado ou gerenciado por controladora WLAN.	Data AP	4
2.17	Permitir a criação de perfis de usuários a partir do qual se determinem parâmetros individuais de QoS, vlan, políticas de firewall e criptografia de tráfego	user guide	139
2.18	Deverá implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF.	user guide	139
2.19	O ponto de acesso poderá estar diretamente ou remotamente conectado ao controlador WLAN, inclusive via roteamento da camada de rede OSI	Data AP	4
2.20	Deverá permitir que o conjunto de pontos de acesso sejam atualizados de forma centralizada pela interface gráfica.	user guide	182
	3 CARACTERÍSTICAS DOS RÁDIOS APS		
3.1	Os pontos de acesso deverão possuir certificado emitido pelo <WIFI Alliance=comprovando os seguintes padrões, protocolos e funcionalidades: IEEE 802.11a; IEEE 802.11b; IEEE 802.11g; IEEE 802.11n; IEEE	WFA129114	1
3.2	Deverá permitir, simultaneamente, usuários configurados nos padrões IEEE 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac e 802.11ax	Datasheet	2
3.3	Implementar as seguintes taxas de transmissão e com fallback automático: IEEE 802.11 a/g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps; IEEE 802.11 b: 11; 5.5; 2 e 1 Mbps; IEEE 802.11n (2.4GHz): MCS0 – MCS15 (6.5 a 300Mbps); IEEE 802.11ac (5GHz): MCS0 – MCS9, (6.5 a 3.467Mbps) para canais de 20/40/80/160MHz; IEEE 802.11ax (2,4GHz): MCS0 – MCS11, (3.6 a 574Mbps) para canais de 20/40MHz; IEEE 802.11ax (5GHz): MCS0 – MCS11, (3.6 a 4.803Mbps) para canais de 20/40/80/160MHz.	Datasheet	2
3.4	Possuir antenas compatíveis com as frequências de rádio dos padrões IEEE 802.11a/n/ac/ax e 802.11/b/g/n com ganho de, pelo menos, 4dBi para frequência de 2.4GHz e 5dBi para frequência de 4.7GHz, com p	Datasheet	2
3.5	Suportar operação em no mínimo: 2x2 MIMO (2.4GHz) e 4x4 MIMO (5GHz);	Datasheet	2

3.6	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.	Datasheet	132
3.7	Possuir capacidade de selecionar automaticamente o canal de transmissão suportando mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2,4 GHz livre pa	cnMaestro	206
3.8	Possibilitar Backup e Restore da configuração por meio da interface gráfica.	cnMaestro	491
3.9	Deverá possuir servidor DHCP interno.	user guide	66
3.10	Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático	user guide	67
3.11	Deverá possuir uma base de usuários interna que diferencie usuários visitantes de funcionários, para ser usada em autenticação 802.1x ou Captive Portal.	user guide	134
3.12	O ponto de acesso deverá permitir a conversão de modo autogerenciado para modo gerenciado por Controlador WLAN através de interface gráfica, em browser padrão (HTTPS), e permitir que todos os demais p	data ap	4
3.13	No modo de funcionamento autogerenciado deverá disponibilizar na interface gráfica informações de usuários conectados, qualidade de sinal e tráfego de dados na rede.	data ap	4
3.14	A potência de transmissão deverá permitir ajuste em intervalos de 1 dBm.	user guide	53
3.15	Possuir capacidade de selecionar automaticamente o canal de transmissão.	user guide	36
3.16	Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.	user guide	36
3.17	Possuir potência de transmissão de, no mínimo, 18 dBm para IEEE 802.11a/b/g/n/ac/ax.	Datasheet	2
3.18	Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras.	user guide	65
3.19	Possuir, uma interface IEEE 802.3bz 100/1000/2500BaseT Ethernet, auto-sensing, auto MDI/MDX.	Datasheet	2
3.20	Possuir, uma interface IEEE 802.3 10/100/1000BaseT Ethernet, auto-sensing, auto MDI/MDX.	Datasheet	2
3.21	Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono).	user guide	182
3.22	Possuir porta de console para gerenciamento e configuração via linha de comando CLI com conector RJ-45, conector padrão RS-232 ou USB ou conexão via Bluetooth para gerenciamento e configuração, difere	user guide	194
3.23	Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível.	user guide	255
3.24	Deverá configurar-se automaticamente ao ser conectado na rede.	user guide	210
3.25	Possuir LED’s indicativos do estado de operação, da atividade do rádio e da interface Ethernet.	user guide	19
3.26	Possuir estrutura que permita fixação do equipamento em teto e parede, e deverá ser fornecido todos os acessórios para que possa ser feita a fixação.		ok

3.27	Deverá ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, documentação técnica e manuais (podendo ser página de internet oficial do fabrica		ok	
3.28	Deverá suportar filtro de conteúdo.			
3.29	Deverá implementar firewall com capacidade de rastreio do estado da conexão (stateful firewall).	user guide		138
3.30	Deverá permitir a criação de políticas de firewall em camada 7 e sua associação de forma dinâmica de acordo com a identidade do usuário autenticado com o ponto de acesso operando no modo autogerenciad	user guide		138
3.31	Deverá implementar mecanismos para controle e priorização de aplicações em Camada 7. Caso o equipamento não realize esta função, deverá ser fornecido solução que realize a priorização e controle de ap	user guide		138
3.32	Implementar varredura de RF nas frequências de 2.4GHz e 5GHz para identificação de Pontos de Acesso intrusos não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso e nos dema	user guide		44
3.33	Permitir o bloqueio da configuração do ponto de acesso via rede wireless.	user guide		271
3.34	Implementar IEEE 802.1x, com pelo menos os seguintes métodos EAP: EAP-FAST, EAP-TLS, PEAP-GTC, PEAP-MSCHAPv2.	Datasheet		3
3.35	Permitir a integração com RADIUS Server com suporte aos métodos EAP citados.	user guide		126
3.36	Implementar protocolo de autenticação para controle do acesso administrativo ao equipamento com mecanismos de AAA.	user guide		125
3.37	Implementar criptografia do tráfego local.	user guide		64
3.38	Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário.	user guide		194
3.39	Implementar WPA com algoritmo de criptografia TKIP e MIC.	user guide		58
3.40	Implementar WPA2 com algoritmo de criptografia AES, 128/256 bits, IEEE 802.11i.	user guide		34
3.41	Implementar WPA3 com CNSA option, Personal (SAE) e Enhanced Open (OWE).	user guide		58
3.42	Implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi- Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) Advanced Encryption Standard	user guide		58
3.43	Deverá possuir modo dedicado de funcionamento de análise de espectro das faixas de frequência de 2.4 e 5 GHz identificando fontes de interferência nessas faixas.	user guide		188
3.44	Deverá possibilitar análise de espectro nos canais em que estiver provendo acesso, sem desconectar os usuários.	user guide		188
3.45	Deverá disponibilizar informações gráficas de análise de espectro em conjunto com o controlador WLAN.	user guide		189
3.46	Deverá suportar sua própria autenticação com o controlador via certificado digital.	user guide		81
3.47	Deverá ser fornecido com a versão de software mais completa disponível para o equipamento.		ok	
3.48	Deverá ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.		ok	

4 REDE E SERVIÇOS

4.1	Capacidade mínima de 250 (duzentos e cinquenta) usuários wireless simultâneos, sem nenhum tipo de licença adicional.	datasheet	3
4.2	Suporte mínimo para 16 (dezesseis) portas de SSIDs por ponto de acesso.	datasheet	3
4.3	Deverá suportar a configuração de limite de banda (rate limit) por usuário e por SSID.	user guide	578
4.4	Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID.	cnmaestro	87
4.5	Permitir habilitar e desabilitar a divulgação do SSID.	user guide	61
4.6	Implementar diferentes tipos de combinações encriptação/autenticação por SSID.	user guide	64
4.7	Deverá permitir a seleção/uso de servidor de autenticação específico com base no SSID.	user guide	252
4.8	Deverá suportar limitação de banda por grupo de usuários ou SSID.	cnmaestro	163
4.9	Deverá oferecer suporte ao mecanismo de localização e rastreamento de usuários (Location Based Service).	cnmaestro	86
4.10	Deverá implementar mecanismo para otimização de roaming entre pontos de acesso.	cnmaestro	682
4.11	Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através: MAC Address, 802.1x em base Local, Captive Portal, 802.1x em base externa RADIUS ou 802.1x em base extern	cnmaestro	686
4.12	Deverá suportar os recursos de controle de acesso, rede guest, segurança Wi-Fi avançada e gerenciamento de tráfego.	cnmaestro	787
4.13	Permitir a criação de filtros de MAC address de forma a restringir o acesso à rede wireless.	cnmaestro	390
4.14	Deverá implementar autenticação de usuários usando Captive Portal e Hotspot 2.0 ou Wispr	cnmaestro	21
4.15	Implementar associação dinâmica de usuários à VLANs com base nos parâmetros da etapa de autenticação.	cnmaestro	371
4.16	Deverá suportar VLANs conforme o padrão IEEE 802.1Q	cnmaestro	556
	ITEM 2 - Controladora Wireless Virtual (Caso a solução exija controladora, considerar este item)		
	5 CARACTERÍSTICAS GERAIS		
5.1	Suportar plenamente os pontos de acesso do ITEM 1.	cnmaestro	18
5.2	Para controladoras WLAN em solução virtualizada, apontar a compatibilidade com plataforma Microsoft Windows Server 2016 ou superior e ambiente de virtualização MS Hyper-V.	cnmaestro	20
5.3	A solução de gerenciamento deverá ser entregue em pares e deverá suportar a formação de múltiplos nós para proporcionar alta disponibilidade.	cnmaestro	46
5.4	Possibilitar a implementação da redundância do controlador de WLAN, no modo ativo/ativo ou ativo/passivo, com sincronismo automático das configurações entre controladores.	cnmaestro	161
5.5	Em caso de falha, a redundância deverá ser realizada de forma automática sem nenhuma ação do administrador de rede.	cnmaestro	579
5.6	Permitir a importação de plantas baixas em formato digital e permitir a visualização dessas plantas com a localização dos pontos de acesso sem fio, clientes e pontos de acesso não autorizados (Rogue A	cnmaestro	74
5.7	Permitir a gerência e identificação individualizada de cada AP.	cnmaestro	135
5.8	Permitir a alteração em lote das características de configuração de um grupo de equipamentos sem a necessidade de configuração individual de cada dispositivo.	cnmaestro	140

5.9	Permitir a atualização remota de firmwares e arquivos de configuração dos APs.	cnmaestro	678
5.10	Permitir a configuração e gerenciamento por meio de browser padrão (HTTPS).	cnmaestro	933
5.11	Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.	cnmaestro	632
5.12	Permitir o envio de alertas ou alarmes através do protocolo SMTP ou através do software de gerenciamento.	cnmaestro	632
5.13	Administrar a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF).	cnmaestro	264
5.14	Permitir a gravação de eventos em log interno e possibilitar o envio dos logs do	cnmaestro	312
5.15	Balancear automaticamente a carga de usuários através de múltiplos pontos de acesso.	cnmaestro	571
5.16	Deverá implementar mecanismos de inteligência artificial para operações de TI (AIOPS).	https://www.cambiumnetworks.com/resource/cnmaestro-x-assurance/	
5.17	Deverá utilizar a tecnologia AI (inteligência artificial) e ML (Machine Learning) para interpretar eventos e fornecer insights com recomendações para resolução de problemas.	cnmaestro	601
5.18	Possuir capacidade de geração de relatórios ao menos dos seguintes tipos: i) lista dos clientes wireless; ii) lista dos APs; iii) informações de configuração WLAN; iv) utilização da rede.	cnmaestro	312
5.19	A solução deverá possuir gerenciamento centralizado com emissão de relatórios e estatísticas com histórico de utilização de pelo menos 30 (trinta) dias.	cnmaestro	312
5.20	Deverá ser do mesmo fabricante dos pontos de acesso do ITEM 1 para fins de total compatibilidade e gerenciamento unificado da solução.	cnmaestro	18

Documento Digitalizado Público

ANEXO G - Tabela de cumprimento dos requisitos BSB TIC

Assunto: ANEXO G - Tabela de cumprimento dos requisitos BSB TIC
Assinado por: Marcia Marto
Tipo do Documento: DOCUMENTO
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Documento Original

Documento assinado eletronicamente por:

- **Márcia Fernanda de Macedo Marto**, **Empregado - CMSUP - SESEG**, em 30/01/2025 16:47:13.

Este documento foi armazenado no SUAP em 30/01/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.cfmv.gov.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 976737
Código de Autenticação: c5eca44b9d