



PRESIDÊNCIA DA REPÚBLICA
Secretaria - Geral
Secretaria Especial de Administração
Diretoria de Tecnologia
Coordenação - Geral de Infraestrutura Tecnológica e Telecomunicações
Coordenação de Redes de Longa Distância e Telecomunicações

Documento Apêndice A/2020/CORET/CGITT/DITEC/SA

Brasília, de de .

APÊNDICE A
ORDEM DE SERVIÇO

Nº:			
Nome Solicitante:		Área:	
Fone/Ramal:	Data:	Hora:	
Serviço/Atividade:			

Recebido por:	Data:	Hora:
---------------	-------	-------

Descrição do serviço/atividade a ser executada (o que será feito, responsabilidade, entregáveis, prazos):

Responsável pela Execução:		
Início	Data:	Hora:
Término	Data:	Hora:
Gestor:		

Indicador de Atraso dos Projetos ou Ordem de Serviço	(Mecanismo de Cálculo conforme item 5.5.1 TR)
Faixa de Ajuste de Pagamento	
Sanção	

Indicador de Desconformidade de Produto	(Mecanismo de Cálculo conforme item 5.5.2 TR)
Faixa de Ajuste de Pagamento	
Sanção	

Situação da Ordem de Serviço:		() Executada	() Não Executada
Motivo:	() Infraestrutura	() Desistência de Usuário	() Outros
Especificação (outros):			
Visto de Conclusão (Solicitante)		Data:	Hora:

Responsável OS



PRESIDÊNCIA DA REPÚBLICA
Secretaria - Geral
Secretaria Especial de Administração
Diretoria de Tecnologia
Coordenação - Geral de Infraestrutura Tecnológica e Telecomunicações
Coordenação de Redes de Longa Distância e Telecomunicações

Documento Apêndice B/2020/CORET/CGITT/DITEC/SA

Brasília, de de .

APÊNDICE B
TERMO DE RECEBIMENTO PROVISÓRIO

Processo Nº:	
Objeto:	
Nº Contrato:	Nº da OS:
Contratada:	
CNPJ:	Fone:

Por este instrumento, atestamos para fins de cumprimento do disposto no Art. 73, inciso II, alínea “a”, da Lei nº 8.666, de 21 de junho de 1993, que os bens e/ou serviços, relacionados no quadro abaixo, foram recebidos nesta data e serão objeto de avaliação quanto aos aspectos de qualidade, de acordo com os Critérios de Aceitação previamente definidos pelo Termo de Referência da Presidência da República.

Item	Descrição	Identificação	Unidade	Quantidade

Ressaltamos que o recebimento definitivo dos bens e/ou serviços ocorrerá em até 15 (quinze) dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do instrumento contratual proveniente do Termo de Referência.

Brasília/DF, ____ de ____ de ____ .

Gestor do Contrato
SIAPE:

Preposto(a) da CONTRATADA

CPF:



PRESIDÊNCIA DA REPÚBLICA
Secretaria - Geral
Secretaria Especial de Administração
Diretoria de Tecnologia
Coordenação - Geral de Infraestrutura Tecnológica e Telecomunicações
Coordenação de Redes de Longa Distância e Telecomunicações

Documento Apêndice C/2020/CORET/CGITT/DITEC/SA

Brasília, de de .

APÊNDICE C
TERMO DE RECEBIMENTO DEFINITIVO

Processo Nº:	
Objeto:	
Nº Contrato:	Nº da OS:
Contratada:	
CNPJ:	Fone:

Por este instrumento, as partes abaixo identificadas atestam para fins de cumprimento do disposto no Art. 73, inciso II, alínea “b”, da Lei nº 8.666, de 21 de junho de 1993, que os bens e/ou serviços relacionados no quadro abaixo, possuem as quantidades e a qualidade compatível com as condições e exigências constantes do Termo de Referência.

Item	Descrição	Identificação	Unidade	Quantidade

Brasília/DF, ____ de _____ de ____ .

Gestor do Contrato
SIAPE:

Preposto(a) da CONTRATADA
CPF:



PRESIDÊNCIA DA REPÚBLICA

Secretaria – Geral

Secretaria Especial de Administração

Diretoria de Tecnologia

Coordenação - Geral de Infraestrutura Tecnológica e Telecomunicações

Coordenação de Redes de Longa Distância e Telecomunicações

Documento Apêndice D/2020/CORET/CGITT/DITEC/SA

TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO

A _____, doravante designada simplesmente CONTRATADA, inscrita no CNPJ/MF sob o número _____, com sede em _____, neste ato representada pelo Senhor (a) _____, portador (a) da Carteira de Identidade n.º _____, expedida pela (o) _____ e do Cadastro da Pessoa Física, CPF/MF sob o n.º _____, conforme documentação comprobatória de vínculo anexo, nos termos do Contrato n.º _____, compromete-se a observar o presente TERMO DE CONFIDENCIALIDADE, denominada simplesmente CONTRATANTE, em conformidade com as cláusulas que seguem:

1. O objetivo deste Termo de Confidencialidade é prover a necessária e adequada proteção às informações de acesso restrito de propriedade exclusiva da CONTRATANTE, reveladas à CONTRATADA, em função da prestação dos serviços objeto do Contrato n.º ____/____.

2. A expressão “informações de acesso restrito” abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, contendo ela ou não rótulo de classificação quanto ao sigilo, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outros, a que, diretamente ou por meio de seus empregados, prepostos ou prestadores de serviço, venham a CONTRATADA ter acesso em razão da execução do contrato celebrado.

3. A CONTRATADA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa da CONTRATANTE, das informações de acesso restrito reveladas.

4. A CONTRATADA compromete-se a não utilizar de forma diversa da prevista no Contrato n.º ____/____ as informações de acesso restrito reveladas.

5. A CONTRATADA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento próprio.

6. A CONTRATADA determinará a observância deste Termo de Confidencialidade a todos os seus empregados, prepostos e prestadores de serviço que estejam direta ou indiretamente envolvidos com a execução do contrato, ficando ainda responsável pela fiscalização do cumprimento das condições constantes no instrumento firmado.

7. Os empregados, prepostos e prestadores de serviço da CONTRATADA que terão acesso às informações da CONTRATANTE deverão ser imputáveis perante a lei.

8. A CONTRATADA obriga-se a informar imediatamente à CONTRATANTE, por escrito e no prazo máximo de 24 horas, contados a partir da data e horário da ocorrência do incidente, qualquer violação das regras de sigilo estabelecidas neste termo de que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

9. A CONTRATADA devolverá imediatamente à CONTRATANTE, ao término do Contrato, todo e qualquer material de propriedade desta, inclusive registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada de acesso restrito, nos termos do presente Termo de Confidencialidade, a que teve acesso em decorrência do vínculo contratual com a CONTRATANTE.

10. A quebra do sigilo das informações de acesso restrito reveladas, devidamente comprovada, sem autorização expressa da CONTRATANTE, possibilitará a imediata rescisão de qualquer contrato firmado entre a CONTRATANTE e a CONTRATADA, sem qualquer ônus para a CONTRATANTE. Nesse caso, a CONTRATADA estará sujeita, por ação ou omissão, além das eventuais sanções definidas no contrato, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

11. Tendo em vista o princípio da boa-fé objetiva, permanece em vigor o dever de sigilo, tratado no presente Termo de Confidencialidade, após o término da vigência do Contrato.

12. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações de acesso restrito da CONTRATANTE.

Por estar de acordo, a CONTRATADA, por meio de seu representante legal, firma o presente Termo de Confidencialidade, lavrando em duas vias de igual teor e forma.

Brasília-DF, de de 2020.

Nome: (Assinatura da Contratada)

RG:

CPF:

DE ACORDO: (integrantes da equipe técnica da CONTRATADA)

Nome:

Nome:

RG:

RG:



PRESIDÊNCIA DA REPÚBLICA
Secretaria - Geral
Secretaria Especial de Administração
Diretoria de Tecnologia
Coordenação - Geral de Infraestrutura Tecnológica e Telecomunicações
Coordenação de Redes de Longa Distância e Telecomunicações

Documento Apêndice E/2020/CORET/CGITT/DITEC/SA

TERMO DE CIÊNCIA

Processo:
Objeto:
Contrato nº:
Contratada:

Pelo presente instrumento, eu _____, CPF nº _____, RG nº _____, expedida em _____, órgão expedidor ____/____, prestador de serviço, ocupando o cargo de _____ na empresa _____, que firmou Contrato com a Presidência da República, DECLARO, para fins de cumprimento de obrigações contratuais e sob pena das sanções administrativas, civis e penais, que tenho pleno conhecimento de minha responsabilidade no que concerne ao sigilo que deve ser mantido sobre os assuntos tratados, as atividades desenvolvidas e as ações realizadas no âmbito da Presidência da República, bem como sobre todas as informações que, por força de minha função ou eventualmente, venham a ser do meu conhecimento, comprometendo-me a guardar o sigilo necessário a que sou obrigado nos termos da _____ legislação _____ vigente.

DECLARO, ainda, nos termos da Política de Segurança da Informação da Secretaria de Administração, Portaria nº 69 de 16 de junho de 2016, estar ciente e CONCORDO com as condições abaixo especificadas, responsabilizando-me por:

- I. tratar o(s) ativo(s) de informação como patrimônio do Presidência da República;
- II. utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço da Presidência da República;
- III. não utilizar ou divulgar em parte ou na totalidade, as informações de propriedade ou custodiadas, sob qualquer forma de armazenamento, pela Presidência da República sem autorização prévia do gestor ou responsável pela informação;
- IV. contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
- V. utilizar credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas da Presidência da República;
- VI. responder, perante a Presidência da República, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

Cidade/UF, ____ de _____ de ____.

Nome do Funcionário

Cargo

CPF nº

Ciente:

Cidade-UF, ____ de _____ de ____.

Nome do Diretor ou representante legal da empresa

Cargo

CPF nº

ANEXO I
ESPECIFICAÇÃO TÉCNICA MÍNIMA DOS ITENS

2 ESPECIFICAÇÕES TÉCNICAS

2.1 Requisitos Gerais

- 2.1.1 O fabricante deverá ser o mesmo para todos os tipos de controladores e para os Pontos de Acesso fornecidos pela CONTRATADA, para fins de compatibilidade e gerenciamento.
- 2.1.2 O prazo de garantia e assistência técnica deverá ser de 60 meses, contados a partir da data do Termo de Aceitação Definitivo.
- 2.1.3 Todas as licenças necessárias para o perfeito funcionamento de todos os itens deverão ser entregues pela CONTRATADA sem ônus para a CONTRATANTE.
- 2.1.4 A CONTRATADA deverá apresentar, na entrega do equipamento, **certificado**, dentro do prazo de validade, referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto;
- 2.1.5 Os equipamentos deverão ser novos e estar em linha de produção, ou seja, estando em conformidade com a versão mais atual em produção.

2.2 ITENS 01 e 02 – Requisitos Comuns - Controladores WLAN modelos 1 e 2

- 2.2.1 **Não serão aceitos** controladores baseados em computação em nuvem;
- 2.2.2 Implementar **redundância** do controlador de WLAN, no modo **ativo/ativo**, ou **ativo/passivo** com sincronismo automático das configurações entre dois ou mais controladores;
- 2.2.3 O gerenciamento dos controladores em **redundância** deverá ser realizado através de um único endereço IP;
- 2.2.4 Em caso de falha, a **redundância** deverá ser realizada de forma automática sem nenhuma ação do administrador de rede;
- 2.2.5 Na ocorrência de falha, a redundância deverá suportar a quantidade de Pontos de Acesso descritos nos Itens 2.3.2 e 2.4.2, respectivamente;
- 2.2.6 Suportar Pontos de Acesso internos e externos do mesmo fabricante nos padrões IEEE 802.11a/b/g/n/ac/ac wave 2/ax;
- 2.2.7 Prover o gerenciamento centralizado dos Pontos de Acesso de cada campus que sejam do mesmo fabricante ofertados neste processo;
- 2.2.8 Conectar-se diretamente e/ou remotamente aos Pontos de Acesso a serem gerenciados, inclusive via roteamento nível 3 da camada OSI;
- 2.2.9 A comunicação entre o ponto de acesso e a controladora wireless deve poder ser efetuada de forma **criptografada**;
- 2.2.10 Permitir a configuração completa dos Pontos de Acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Radiofrequência (RF);
- 2.2.11 **Ajustar automaticamente a potência** de Pontos de Acesso adjacentes, na ocorrência de inoperância de um ponto de acesso, de modo a minimizar a falta de cobertura em áreas não assistidas;
- 2.2.12 **Ajustar automaticamente os canais** de modo a otimizar a cobertura de rede e alterar as condições de RF baseado em performance;
- 2.2.13 **Detectar interferência** e ajustar parâmetros de RF, evitando problemas de cobertura e controle da propagação indesejada de RF;
- 2.2.14 **Ajustar dinamicamente o nível de potência e canal** de rádio dos Pontos de Acesso, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade;

- 2.2.15 Implementar padrão IEEE 802.11h ou 802.11a;
- 2.2.16 Possibilitar **roaming** com integridade de sessão, dando suporte a aplicações em tempo real, tais como, **VoWLAN** (*Voice over Wireless LAN*) e **streaming** de vídeo;
- 2.2.17 Implementar **Beamforming** e **Fast-Roaming**;
- 2.2.18 Implementar disponibilidade de **SSID baseado em dia da semana e hora**, permitindo ao administrador do sistema, habilitar ou não um determinado SSID somente em hora/dia da semana determinados;
- 2.2.19 Permitir configurar o valor de **Short Guard Interval** ou adaptar de forma automática com base na comunicação entre pontos de acesso e dispositivos cliente;
- 2.2.20 Implementar sistema automático de **balanceamento de carga** para associação de clientes entre **Pontos de Acesso** próximos, para otimizar a performance;
- 2.2.21 Implementar funcionalidade de **balanceamento de carga** entre os **rádios** de um mesmo Ponto de Acesso;
- 2.2.22 Permitir que o serviço wireless seja **desabilitado** de determinado Ponto de Acesso.
- 2.2.23 Permitir selecionar o serviço de qual rádio (banda), de determinado Ponto de Acesso, deve ser **desabilitado**;
- 2.2.24 Permitir que seja definida uma **taxa de transmissão mínima** na qual os clientes devem se conectar, de modo a evitar a degradação da rede;
- 2.2.25 Suportar **802.11e/WMM** (QoS);
- 2.2.26 Possuir funcionalidade de configuração do **limite de banda disponível** por **usuário** ou através de SSID/BSSID;
- 2.2.27 Permitir a configuração de **prioridade de tráfego** de um determinado SSID sobre os outros SSIDs;
- 2.2.28 Implementar suporte aos protocolos IPv4, IPv6 e *dual-stack*;
- 2.2.29 Implementar os protocolos **NTP** ou **SNTP**;
- 2.2.30 Suportar o protocolo **LLDP**;
- 2.2.31 Suportar **tagging** de VLANs;
- 2.2.32 Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE **802.1x**;
- 2.2.33 Suportar associação dinâmica de **ACL e de QoS por usuário**, com base nos parâmetros da etapa de autenticação;
- 2.2.34 Suportar, no mínimo, **512** (quinhentos e doze) **SSIDs** simultâneos;
- 2.2.35 Possuir funcionalidade de **balanceamento de carga** entre **VLANs** e permitir que clientes sejam designados para diferentes VLANs dentro de um mesmo SSID;
- 2.2.36 Permitir o **mapeamento** entre WLANs e VLANs;
- 2.2.37 Permitir que os SSIDs operem em modo de **tunelamento** de tráfego remoto ou **comutação** de tráfego local;
- 2.2.38 Em caso de **falha de comunicação** entre os Pontos de Acesso e a controladora, os usuários associados às redes sem fio devem continuar conectados com acesso à rede. Também deve permitir que novos usuários se associem às redes sem fios utilizando autenticação do tipo 802.1x mesmo que os Pontos de Acesso estejam sem comunicação com a controladora;
- 2.2.39 Permitir a criação de redes wireless **Mesh**;

- 2.2.40 Permitir **restringir o gerenciamento** através de listas de controle de acesso com no mínimo as seguintes opções: endereço IP, intervalo de IPs, ou sub-redes pré-configuradas;
- 2.2.41 Permitir a configuração e o gerenciamento através de rede IP utilizando interface de **gerenciamento WEB** acessível de forma segura em browser padrão (HTTPS) e por meio de interface de gerenciamento via **linha de comando** (CLI) utilizando sua porta console ou conexão SSH;
- 2.2.42 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;
- 2.2.43 Deve permitir a **atualização de software** dos Pontos de Acesso de modo centralizado via WEB;
- 2.2.44 Implementar **backup e recuperação das configurações** dos Pontos de Acesso, com a possibilidade de verificar diferenças entre versões. Implementar ainda a realização de agendamento de backup de forma diária, semanal e mensal com a possibilidade de salvar as configurações em servidor FTP ou TFTP;
- 2.2.45 Possuir capacidade de **alteração em lote** das características de configuração de um grupo de equipamentos sem a necessidade de configuração individual de cada dispositivo;
- 2.2.46 Implementar **agendamento de tarefas** de configuração com o registro de *log* do resultado da tarefa;
- 2.2.47 **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;
- 2.2.48 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, dados de associação e de autenticação 802.1x;
- 2.2.49 Armazenar **informações históricas sobre autenticação** de usuários da rede sem fio, tanto da rede corporativa (802.1x) como da rede *guest (captive portal)*;
- 2.2.50 Permitir a **localização de endereço IP** e de endereço MAC na infraestrutura de rede sem fio;
- 2.2.51 Possibilitar a configuração de envio dos eventos do Controlador WLAN para um servidor de **Syslog remoto**;
- 2.2.52 Implementar, pelo menos, os padrões abertos de gerência de rede **SNMPv2c** e **SNMPv3**, incluindo a geração de *traps* SNMP;
- 2.2.53 Implementar **MIB privativa** que forneça informações relativas ao funcionamento do equipamento;
- 2.2.54 Permitir a **visualização de alertas** da rede em tempo real;
- 2.2.55 Implementar no mínimo dois **níveis de acesso administrativo** ao equipamento (apenas leitura e leitura/escrita) protegidos por senhas independentes;
- 2.2.56 Permitir a **customização do acesso administrativo** através de atribuição de grupo de função do usuário administrador;
- 2.2.57 Permitir o **envio de alertas ou alarmes** através do protocolo **SMTP**, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS);
- 2.2.58 Permitir que o processo de **atualização de versão** seja realizado através de *browser* padrão (HTTPS) ou SSH;

- 2.2.59 Possuir a capacidade de **importação de certificados digitais** emitidos por uma autoridade certificadora externa;
- 2.2.60 Possuir **ferramentas de diagnóstico** e *log* de eventos para depuração e gerenciamento em primeiro nível;
- 2.2.61 Possuir **ferramentas de diagnóstico** de problemas de conexão/autenticação dos clientes wireless;
- 2.2.62 Implementar a **verificação de consumo** de memória, CPU e links, com a definição de limites máximos, de forma que quando ultrapassados, a plataforma gere alerta de aviso;
- 2.2.63 Possuir a capacidade de geração de informações em tempo real ou **relatórios históricos** de no mínimo os seguintes tipos:
 - 2.2.63.1 Sessões de clientes wireless;
 - 2.2.63.2 Clientes conectados por tipo de autenticação;
 - 2.2.63.3 Clientes conectados por ponto de acesso;
 - 2.2.63.4 Clientes conectados por canal;
 - 2.2.63.5 Clientes conectados por potência do sinal;
 - 2.2.63.6 Largura de banda utilizada por cliente;
 - 2.2.63.7 Largura de banda utilizada por ponto de acesso;
 - 2.2.63.8 Largura de banda total utilizada;
 - 2.2.63.9 Estado do ponto de acesso (*online/offline*);
 - 2.2.63.10 Inventário dos Pontos de Acesso (hardware e software);
 - 2.2.63.11 Relação sinal-ruído;
 - 2.2.63.12 Potência de sinal;
 - 2.2.63.13 Eventos e alarmes.
- 2.2.64 Suportar os seguintes **métodos de descoberta** de novos Pontos de Acesso:
 - 2.2.64.1 De maneira manual baseado em IP estático;
 - 2.2.64.2 De maneira automática baseado em DHCP;
 - 2.2.64.3 De maneira automática baseado em DNS;
 - 2.2.64.4 De maneira automática baseado em *broadcast*.
- 2.2.65 Implementar **análise de tráfego** por WLAN, por Ponto de Acesso e por dispositivo cliente, apresentando os 10 itens mais usados;
- 2.2.66 Suportar a **identificação de aplicações comuns de mercado** utilizadas pelos dispositivos clientes conectados aos Pontos de Acesso, com base na camada 7 do modelo OSI, permitindo também o bloqueio e o controle de banda (*uplink* e/ou *downlink*), acesso e definição de regra de QoS para estas aplicações;
- 2.2.67 Permitir **visualizar a localização dos Pontos de Acesso** e através desta obter o status de funcionamento dos mesmos;
- 2.2.68 Possibilitar a **importação de plantas baixas** nos formatos **dwg** ou **jpg** ou **png**, devendo permitir a visualização dos Pontos de Acesso instalados, com seu estado de funcionamento;
- 2.2.69 Disponibilizar **mapas gráficos de rádio frequência** (*heat maps*) para apresentar a situação atual do espectro e dos Pontos de Acesso;

- 2.2.70 Implementar **funcionalidade de análise espectral**, permitindo a detecção de interferências no ambiente de rede sem fio, gerando alarmes das interferências detectadas;
- 2.2.71 Suportar de forma centralizada a **autenticação de usuários** através de integração com servidores AAA;
- 2.2.72 Deverá possuir **base de dados interna de usuários** com suporte a pelo menos 4 (quatro) mil usuários;
- 2.2.73 Suportar no mínimo os seguintes servidores ou **meios de autenticação** AAA: Microsoft Active Directory, LDAP e RADIUS;
- 2.2.74 Suportar o mecanismo de **contabilidade** (*accounting*) para os servidores RADIUS;
- 2.2.75 Permitir a seleção/uso de servidor **RADIUS** específico com base no SSID;
- 2.2.76 Suportar servidor de autenticação **RADIUS redundante**. Isto é, na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário;
- 2.2.77 Suportar a criação de uma **zona de visitantes**, que terão seu acesso controlado através de senha cadastrada internamente, sendo que este deverá possuir a configuração de tempo pré-determinado de acesso a rede wireless;
- 2.2.78 Permitir a criação de **múltiplos usuários visitantes** (*guests*) de uma única vez (em lote);
- 2.2.79 Permitir que, após o processo de autenticação de usuários visitantes (*guests*), os **usuários sejam redirecionados** para uma página de navegação específica e configurável;
- 2.2.80 Implementar **autenticação via portal web** (*captive portal*) para os usuários que não puderem se autenticar via 802.1x;
- 2.2.81 Permitir a utilização de **portal web** (*captive portal*) **externo** à controladora;
- 2.2.82 Permitir que o **Portal web** para usuários visitantes (*guest*) seja **personalizável**, com a inclusão de imagens;
- 2.2.83 Permitir a configuração do número máximo de conexões simultâneas realizadas por uma mesma conta visitante, possibilitando que um usuário possua mais de um dispositivo na rede com a mesma senha e que contas visitantes coletivas sejam utilizadas em eventos;
- 2.2.84 Permitir que múltiplos usuários visitantes (*guests*) **compartilhem a mesma senha** de acesso à rede;
- 2.2.85 Permitir **enviar a senha** de usuários visitantes (*guests*), por **e-mail**;
- 2.2.86 Permitir o **encaminhamento do tráfego** de saída de usuários visitantes (*guests*) diretamente **para a internet**, de forma totalmente separada do tráfego da rede corporativa;
- 2.2.87 Permitir o **isolamento do tráfego** entre usuários visitantes (*guests*) em uma mesma VLAN/Subnet;
- 2.2.88 Deverá ser possível especificar o tipo de **serviço Bonjour** que será permitido entre VLANs;
- 2.2.89 Suportar **mecanismo de acesso** de acordo com o padrão **Hotspot 2.0/Passpoint**;
- 2.2.90 Implementar, pelo menos, os seguintes **padrões de segurança** wireless:
 - 2.2.90.1 (WPA) Wi-Fi *Protected Access*;
 - 2.2.90.2 (WPA2) Wi-Fi *Protected Access 2 (Personal e Enterprise)*;
 - 2.2.90.3 (WPA3) Wi-Fi *Protected Access 2 (Personal e Enterprise)*;
 - 2.2.90.4 (TKIP) *Temporal Key Integrity Protocol*;

- 2.2.90.5 (AES) *Advanced Encryption Standard*;
- 2.2.90.6 IEEE 802.1x;
- 2.2.90.7 IEEE 802.11i;
- 2.2.90.8 IEEE 802.11w.
- 2.2.91 Implementar, pelo menos, os seguintes **controles e filtros**:
 - 2.2.91.1 L2 – Baseado em MAC *Address* e *Client Isolation*;
 - 2.2.91.2 L3 – Baseado em Endereço IP;
 - 2.2.91.3 L4 – Baseado em Portas TCP/UDP;
 - 2.2.91.4 Baseado em protocolo;
 - 2.2.91.5 Baseado em sistema operacional do dispositivo.
- 2.2.92 Permitir a **autenticação para acesso** dos usuários conectados nas redes WLAN (Wireless) mediante:
 - 2.2.92.1 MAC *Address*;
 - 2.2.92.2 Autenticação Local;
 - 2.2.92.3 *Captive Portal*;
 - 2.2.92.4 *Active Directory*;
 - 2.2.92.5 RADIUS;
 - 2.2.92.6 IEEE 802.1x;
 - 2.2.92.7 LDAP.
- 2.2.93 Possuir mecanismos de *Wireless Intrusion Protection* para redes 802.11;
- 2.2.94 Possuir todos os **recursos e licenças** necessários para prevenir no mínimo os seguintes tipos de ataques:
 - 2.2.94.1 Rogue AP ou similares;
 - 2.2.94.2 *AP Spoofing* ou similares (APs não pertencentes ao controlador propagando a mesma SSID);
 - 2.2.94.3 MAC Spoofing (APs não pertencentes ao controlador propagando o mesmo MAC de um AP válido);
- 2.2.95 Implementar **varredura de RF contínua**, programada ou sob demanda nas bandas IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, 802.11n e 802.11x para identificação de ataques e Pontos de Acesso intrusos não autorizados (*rogues*) ou clientes irregulares;
- 2.2.96 Utilizar os Pontos de Acesso para fazer a **monitoração do ambiente** Wireless procurando por Pontos de Acesso do tipo **rogue** de forma automática;
- 2.2.97 Implementar **mecanismos para detecção** de Pontos de Acesso do tipo **rogue** com informações de no mínimo:
 - 2.2.97.1 AP não pertencentes ao controlador propagando a mesma SSID;
 - 2.2.97.2 AP não pertencentes ao controlador propagando o mesmo MAC de um AP válido;
 - 2.2.97.3 *Rogue AP* – AP não pertencentes ao controlador;
 - 2.2.97.4 AP não pertencentes ao controlador exibindo qualquer SSID pertencentes ao mesmo segmento de rede LAN;
 - 2.2.97.5 AD HOC – Detecção de redes AD HOC.

- 2.2.98 Implementar **mecanismo de contenção** de Pontos de Acesso do tipo **rogue**, com a opção de envio de pacotes 802.11 de **desautenticação** para os clientes conectados em tais Pontos de Acesso;
- 2.2.99 Implementar mecanismo de **identificação de Pontos de Acesso amigáveis** (através do *MAC Address* ou *SSID*), que não fazem parte da solução, mas que não são Pontos de Acesso *rogue*, portanto não seriam passíveis de contenção;
- 2.2.100 Suportar integração com *tags* da **Ekahau** e **AeroScout**/Stanley para *Real-Time Location Service* (RTLS);
- 2.2.101 Permitir que que clientes da rede sem fio tenham o acesso desabilitado ou removido (por usuário ou *MAC Address*) em casos de incidentes de segurança.

2.3 ITEM 01 - Requisitos específicos ao controlador WLAN modelo 01

- 2.3.1 Será aceito apenas controladores do tipo **appliance físico**. Não será aceito *appliance* do tipo virtual;
- 2.3.2 Capacidade para gerenciar no mínimo **50 (cinquenta)** Pontos de Acesso simultâneos;
- 2.3.3 Suportar, no mínimo, **500 (quinhentos)** usuários simultâneos;
- 2.3.4 Possuir porta de console para gerenciamento e configuração via linha de comando CLI com conector RJ-45 ou conector padrão RS-232 ou USB;
- 2.3.5 Possuir, pelo menos, 02 (duas) portas, pelo menos, do tipo Gigabit Ethernet 10/100/1000 BASE-T para controle dos Pontos de Acesso;
- 2.3.6 Possuir 01 (uma) interface RJ45 ou serial exclusiva para gerenciamento;
- 2.3.7 Possuir LEDs para a indicação da situação (status) de atividade do equipamento e das portas Ethernet;
- 2.3.8 Possuir fonte de alimentação com seleção automática de tensão (110 - 240VAC);
- 2.3.9 Deverá possuir hardware dedicado com software de gerenciamento e administração embarcado;
- 2.3.10 Não serão aceitas soluções baseadas nas premissas de computação virtual sem hardware dedicado;
- 2.3.11 O hardware e software deverão ser do mesmo fabricante para garantir completa compatibilidade da solução;
- 2.3.12 Deve suportar temperatura de operação entre 0°C a 40°C;
- 2.3.13 Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de energia elétrica, documentações técnicas e manuais que contenham informações suficientes, que possibilite a instalação, configuração e operacionalização do equipamento;
- 2.3.14 Deve vir acompanhado de todos os acessórios e cabos para instalação em rack padrão de 19",

2.4 ITEM 02 – Requisitos específicos ao controlador WLAN modelo 02

- 2.4.1 Controlador do tipo *appliance* físico;
- 2.4.2 Capacidade para gerenciar no mínimo **250 (duzentos e cinquenta)** Pontos de Acesso simultâneos;
- 2.4.3 Suportar, no mínimo, **4.000 (quatro mil)** usuários simultâneos;
- 2.4.4 Possuir porta de console para gerenciamento e configuração via linha de comando CLI com conector RJ-45 ou conector padrão RS-232 ou USB;
- 2.4.5 Possuir, pelo menos, 02 (duas) portas do tipo Gigabit Ethernet 10/100/1000 BASE-T para controle dos Pontos de Acesso;
- 2.4.6 Possuir 01 (uma) interface RJ45 ou serial exclusiva para gerenciamento;
- 2.4.7 Possuir LEDs para a indicação da situação (status) de atividade do equipamento e das portas Ethernet;
- 2.4.8 Possuir fonte de alimentação com seleção automática de tensão (110 - 240VAC);
- 2.4.9 Deverá possuir hardware dedicado com software de gerenciamento e administração embarcado;
- 2.4.10 Não serão aceitas soluções baseadas nas premissas de computação virtual sem hardware dedicado;
- 2.4.11 O hardware e software deverão ser do mesmo fabricante para garantir completa compatibilidade da solução;
- 2.4.12 Deve suportar temperatura de operação entre 0°C a 40°C;
- 2.4.13 Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de energia elétrica, documentações técnicas e manuais que contenham informações suficientes, que possibilite a instalação, configuração e operacionalização do equipamento;
- 2.4.14 Deve vir acompanhado de todos os acessórios e cabos para instalação em rack padrão de 19”,

2.5 ITEM 03 - Ponto de Acesso Indoor

- 2.5.1 O equipamento deverá ser do tipo Ponto de Acesso com operação no modo gerenciado por controladora de Rede WLAN e no modo auto gerenciado;
- 2.5.2 Possuir certificado de conformidade técnica de produto do tipo Transceptor de Radiação Restrita, emitido pela Anatel;
- 2.5.3 Equipamento ponto de acesso para rede local sem fios deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ac Wave 2 e IEEE802.11ax com operação nas frequências **2.4 GHz e 5 GHz** de forma simultânea;
- 2.5.4 Ser do mesmo fabricante do Controlador WLAN, para fins de compatibilidade e gerenciamento;
- 2.5.5 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;
- 2.5.6 Ser apresentado **certificado** válido de **interoperabilidade** fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point;

- 2.5.7 Ser compatível com o **padrão UL 2043 ou UL 60950-1**, que regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça;
- 2.5.8 Implementar o protocolo de enlace **CSMA/CA** (*Carrier Sense Multiple Access/Collision Avoidance*) e operar nas modulações **DSSS** e **OFDM**;
- 2.5.9 Possuir **antenas internas e integradas** com padrão de irradiação **omnidirecional** compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ac Wave2 e IEEE802.11ax com ganhos de, no mínimo 1 dBi para 2.4GHz e 2 dBi para 5GHz;
- 2.5.10 **Não serão aceitos equipamentos com antenas aparentes** (externas ao ponto de acesso) que sejam rosqueáveis, permitindo a remoção das antenas;
- 2.5.11 Suportar **potência de saída** de no mínimo 19 dBm nas frequências de 2.4 e 5 GHz;
- 2.5.12 Atender aos padrões IEEE 802.11d e 802.11k;
- 2.5.13 Suportar **canalização** de 20 MHz, 40 MHz e 80 MHz;
- 2.5.14 Possuir suporte a *Single User* MIMO (SU-MIMO) e *Multi User* MIMO (MU-MIMO) no mínimo 4x4 com 4 *spatial streams* e, 5GHz e no mínimo 2x2 com 2 *spatial streams* em 2.4GHz;
- 2.5.15 Suportar mecanismo que identifique e associe clientes **preferencialmente** na banda de **5GHz**, deixando a banda de 2,4 GHz livre para dispositivos que trabalhem somente nesta frequência;
- 2.5.16 Possuir 2 (**duas**) interfaces, com no mínimo **1 GbE**, utilizando conector RJ-45, para conexão à rede local;
- 2.5.17 Possuir **indicadores físicos** para a indicação do status de: portas ethernet, rede wireless, gerenciamento via controladora e atividades do equipamento;
- 2.5.18 Possibilitar alimentação elétrica local via **fonte de alimentação** com seleção automática de tensão (100-240V) e via padrão **PoE** (IEEE 802.3af ou 802.3at) usando porta de no mínimo **1GbE**;
- 2.5.19 Suportar **temperatura de operação** entre 0°C a 40°C com PoE ativado;
- 2.5.20 Possuir estrutura que permita a utilização do equipamento em **locais internos**, com fixação em teto e parede;
- 2.5.21 Ser fornecido com a **versão** mais recente do **software** interno dos Pontos de Acesso;
- 2.5.22 Ser fornecido com todas as **funcionalidades** de segurança **instaladas**. Não deve haver licença restringindo itens de segurança do equipamento e nem a quantidade de usuários conectados;
- 2.5.23 Ser fornecido com **todas as licenças** para funcionamento em **MESH** (WiFi *Mesh*);
- 2.5.24 Suportar a utilização de **sistema antifurto** do tipo *Kensington lock* ou similar que permita a instalação de um cabo de segurança e/ou cadeado com a finalidade de evitar furto do equipamento;
- 2.5.25 Permitir a **configuração e gerenciamento** direto através de **browser** padrão (HTTPS), **SSH**, **SNMPv2c** e **SNMPv3**, ou através do controlador, a fim de se garantir a segurança dos dados;
- 2.5.26 Implementar funcionamento em **modo gerenciado** por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF;

- 2.5.27 Permitir que sua **configuração** seja **automaticamente** realizada quando este for conectado no ambiente de rede do Controlador WLAN especificado neste documento;
- 2.5.28 O Ponto de Acesso poderá estar diretamente ou remotamente conectado ao controlador WLAN, inclusive via roteamento da camada 3 de rede OSI;
- 2.5.29 O Ponto de Acesso deverá **conectar-se** ao controlador WLAN **através de túnel** seguro padrão ou através de protocolo de comunicação seguro que ofereça controle total do equipamento;
- 2.5.30 Permitir **ajustes dinâmicos de RF** modo a otimizar o tamanho da célula de abrangência de RF;
- 2.5.31 Permitir que o **processo de atualização de versão** seja realizado manualmente através da WEB ou FTP ou TFTP e automaticamente através do Controlador WLAN descrito neste documento;
- 2.5.32 Implementar **cliente DHCP**, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático;
- 2.5.33 Suportar **VLANs** seguindo a norma IEEE 802.1q;
- 2.5.34 Suportar **associação dinâmica de usuários** à VLANs de acordo com parâmetros de autenticação na rede wireless;
- 2.5.35 Possuir suporte a pelo menos **16 SSIDs** por Ponto de Acesso;
- 2.5.36 Permitir habilitar e desabilitar a **divulgação do SSID**;
- 2.5.37 Possuir capacidade de **selecionar automaticamente o canal** de transmissão;
- 2.5.38 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;
- 2.5.39 Suportar técnicas de **qualidade de serviço** de extensões multimídia **WME e WMM**;
- 2.5.40 Suportar, no mínimo, **250 usuários** wireless simultâneos;
- 2.5.41 Suportar, no mínimo, **30 usuários de voz** sobre wireless simultâneos;
- 2.5.42 Possuir capacidade de **processamento** de, no mínimo, 600 Mbit/s em 2.4GHz e, no mínimo, 1.7Gbit/s em 5 GHz;
- 2.5.43 Implementar as seguintes **taxas de transmissão** mínimas com *fallback* automático:
 - 2.5.43.1 IEEE 802.11b: 11, 5.5, 2 e 1 Mbps;
 - 2.5.43.2 IEEE 802.11a e IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;
 - 2.5.43.3 IEEE 802.11n: 6.5 Mbps – 600 Mbps;
 - 2.5.43.4 IEEE 802.11ac: 6.5 Mbps – 1733 Mbps.
- 2.5.44 Deverá permitir a criação de **filtros de MAC Address** de forma a restringir o acesso à rede wireless;
- 2.5.45 Funcionar via configuração do controlador no modo **MESH (WiFi Mesh)** **sem adição de novo hardware** ou alteração do sistema operacional, sendo a comunicação até o controlador efetuada via wireless ou por pelo menos 02 pontos ethernet conectados ao controlador ou a uma rede local;
- 2.5.46 Permitir **configurar individualmente para cada SSID** se o tráfego será distribuído pelo túnel até a controladora ao qual ele está registrado e se será comutado localmente no Ponto de Acesso;
- 2.5.47 Implementar, em conjunto com o controlador WLAN, **associação dinâmica de usuário a VLAN**, com base nos parâmetros de autenticação;

- 2.5.48 Implementar a tecnologia de **Beamforming** para melhorar o desempenho de transmissão de dados para determinados usuários da rede sem fio;
- 2.5.49 Implementar **MRC** – *Maximum Ratio Combining* ou similar;
- 2.5.50 Implementar, pelo menos, os **seguintes padrões de segurança wireless**:
 - 2.5.50.1 (WPA) *Wi-Fi Protected Access*;
 - 2.5.50.2 (WPA2) *Wi-Fi Protected Access 2 (Personal e Enterprise)*;
 - 2.5.50.3 (WPA3) *Wi-Fi Protected Access 3 (Personal e Enterprise)*;
 - 2.5.50.4 (AES) *Advanced Encryption Standard*;
 - 2.5.50.5 (TKIP) *Temporal Key Integrity Protocol*;
 - 2.5.50.6 IEEE 802.1x;
 - 2.5.50.7 IEEE 802.11i;
 - 2.5.50.8 IEEE 802.11w.
- 2.5.51 Permitir, em conjunto com o controlador WLAN, a **integração** com **RADIUS Server** ou Microsoft **Active Directory** para autenticação de usuários;
- 2.5.52 Implementar, em conjunto com o controlador, **varredura de RF** nas bandas 802.11a, 802.11b/g, 802.11n, 802.11ac e 802.11ax para identificação de Pontos de Acesso **intrusos** não autorizados (*rogues*) e **interferências no canal** habilitado ao ponto de acesso e nos demais canais configurados na rede WLAN, sem impacto no seu desempenho;
- 2.5.53 Permitir **controle e gerenciamento** pelo controlador WLAN através de **Camada 2 ou 3** do modelo OSI;
- 2.5.54 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 rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1x mesmo que os Pontos de Acesso estejam sem comunicação com a controladora;
- 2.5.55 Deve suportar, somente por meio do Ponto de Acesso em conjunto com o controlador de rede sem fio, a **identificação e controle de aplicações** dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI;
- 2.5.56 Implementar **mecanismo para otimização** de *roaming* entre Pontos de Acesso;
- 2.5.57 Suportar *HotSpot 2.0*, *Captive Portal* e WISPr;
- 2.5.58 Suportar, em conjunto com o controlador de rede sem fio, a **configuração de limite de banda** (*rate limit*) por usuário ou por SSID;
- 2.5.59 Oferecer suporte ao mecanismo de **localização e rastreamento de usuários** (*Location Based Service*);
- 2.5.60 Permitir a criação de **ACLs** de Camada 3 e 4 do modelo OSI;
- 2.5.61 Deverá ser possível criar **políticas de controle** com base no tipo de sistema operacional do dispositivo;
- 2.5.62 Suportar funções para **análise de espectro**.

2.6 ITEM 05 - Serviços de instalação e configuração

- 2.6.1 Fazem parte da configuração e testes os itens 1, 2 e 3.
- 2.6.2 Fazem parte da instalação os itens 1 e 2.

- 2.6.3 A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes, respeitando os prazos definidos para entrega e instalação, e executados por técnico com certificação oficial do fabricante, compatível com o objeto deste processo.
- 2.6.4 A comprovação da certificação oficial do fabricante deverá ser apresentada no momento da assinatura do contrato.
- 2.6.5 O Serviço de instalação deve considerar no mínimo a migração dos SSIDs e configurações das controladoras existentes. Além disso, deve ser realizada ativação das funcionalidades de autenticação (*captive portal*) utilizando base RADIUS ou LDAP (bases existentes na PR);
- 2.6.6 Os produtos deverão ser entregues, instalados e configurados nas dependências da Presidência da República (Brasília/DF), nos endereços listados no Termo de Referência;
- 2.6.7 Os parâmetros pré-configurados pelo fabricante deverão ser alterados de forma a prover maior segurança aos dispositivos instalados. A CONTRATADA deverá identificar os parâmetros que precisam ser alterados (ex. SSID, senhas de acesso e configuração, endereços específicos, comunidade SNMP etc.) e propor, na documentação a ser apresentada à CONTRATANTE, os novos valores para esses parâmetros;
- 2.6.8 Softwares de terceiros que porventura sejam necessários para a implantação da solução também deverão ser instalados e configurados pela CONTRATADA;
- 2.6.9 A instalação **não contempla a substituição dos Pontos de Acesso** da solução atual pelos Pontos de Acesso a serem adquiridos neste documento;
- 2.6.10 O projeto e cronograma dos serviços de instalação, devem ser documentados e fornecidos à CONTRATANTE em até 20 dias úteis contados da assinatura do contrato, contendo no mínimo os seguintes itens para cada local de instalação:
 - 2.6.10.1 Data de início e término da instalação, incluindo o repasse de informações *Hands-on*;
 - 2.6.10.2 Nome completo e número de identidade de todos os técnicos que executarão os serviços;
 - 2.6.10.3 Relação dos materiais (hardware, software e licenças) que compõem as entregas;
 - 2.6.10.4 Detalhamento da configuração, plano de migração, ativação, reversão e contingência.
- 2.6.11 A CONTRATANTE realizará a avaliação do Projeto e Cronograma de Instalação, em até **10 dias úteis**, apontando eventuais ajustes no projeto ou planejamento, devendo a CONTRATADA realizar as adequações necessárias no documento em até **10 dias úteis**;
- 2.6.12 Após aprovação do projeto de implantação e cronograma, a CONTRATADA poderá iniciar as instalações, prosseguindo com os prazos estabelecidos pela CONTRATANTE;
- 2.6.13 Após a instalação de cada fase, o desempenho e condições da solução devem ser monitorados (*in-loco*) pelo prazo mínimo de 2 (dois) dias consecutivos, exceto feriados e finais de semana, de 08:00 a 19:00 horas, afim de avaliar possíveis problemas ou não conformidades na operação;
- 2.6.14 Ao término dos serviços deverá ser realizado e entregue o backup das configurações, bem como um relatório detalhado para posterior continuidade e manutenção da solução instalada, contendo todos os itens configurados no projeto (relatório *as-built*), incluindo:
 - 2.6.14.1 Listagem das configurações dos equipamentos com comentários sobre os principais comandos e as justificativas dos parâmetros utilizados;
 - 2.6.14.2 Todos os usuários e endereços de acesso;
 - 2.6.14.3 Endereços de rede e VLANs ID configurados em cada porta do equipamento;

- 2.6.14.4 Números de séries, data da finalização da instalação e data de vencimento da garantia;
- 2.6.14.5 Endereço web para acesso a documentação oficial, registro no canal de suporte do fabricante e telefone de contato e e-mail para o suporte direto com o fornecedor;
- 2.6.14.6 Ao término de todas as instalações, a CONTRATADA deverá comunicar a CONTRATANTE a conclusão e solicitar o Termo de Recebimento Provisório.
- 2.6.14.7 Em até 10 (dez) dias da emissão do Termo de Recebimento Provisório, depois de finalizada a instalação e a configuração dos dispositivos, deverá ser feito **teste de aceitação** pela CONTRATANTE, auxiliado pela CONTRATADA, a fim de garantir que todos os requisitos e funcionalidades solicitados estão implementados e operacionais. Sendo confirmada a operação e desempenho satisfatório de todos equipamentos e serviços, nos termos das especificações técnicas do Termo de Referência, a CONTRATANTE emitirá o Termo de Recebimento Definitivo.
- 2.6.15 A CONTRATADA assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio da Presidência da República ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando da entrega, instalação e configuração da solução, na área de prestação dos serviços, mesmo que fora do exercício das atribuições previstas no contrato;
- 2.6.16 Os empregados da CONTRATADA envolvidos na implantação da solução, embora sujeitos a normas disciplinares ou convencionais da Presidência da República, não terão qualquer vínculo empregatício com a CONTRATANTE;
- 2.6.17 As informações referentes à solução implantada, bem como acerca das instalações da Presidência da República, são proprietárias, sendo vedada qualquer divulgação sem prévia autorização, cabendo penalizações administrativas e sanções legais cabíveis, em caso de descumprimento;
- 2.6.18 Ao final da instalação, a CONTRATADA deverá entregar toda a documentação que descreva os processos de instalação e configuração dos produtos fornecidos, detalhes de implementação e diagramas topológicos (as-built). O documento deverá conter, ainda, marca, modelo, número de série e local de instalação de todos os equipamentos e comprovação de garantia para todos os produtos, por todo o período contratado. Na ocasião, a versão final da documentação revisada e aceita pela Presidência da República deverá ser apresentada à equipe técnica da CONTRATANTE quando da finalização da instalação e configuração;
- 2.6.19 A coordenação do processo de instalação dos equipamentos, bem como a instalação do software de gerência, deverá ser executada por técnico certificado pelo fabricante, capacitado para o projeto e a instalação de redes wireless. O certificado deverá ser apresentado à CONTRATANTE como pré-requisito para o início dos trabalhos de instalação;
- 2.6.20 O processo de instalação e implantação da solução será acompanhado e supervisionado pela CONTRATANTE, a quem a CONTRATADA deverá se reportar antes de qualquer ação e decisão referente à implantação da solução.

2.7 ITEM 06 - Treinamento

- 2.7.1 Treinamento com, no mínimo, 30 (trinta) horas de duração, a ser ministrado por videoconferência para até 15 (quinze) servidores localizados na Presidência da República, em turmas de no mínimo 5 (cinco) participantes, em horário comercial, com carga horária de, no máximo, 4 (quatro) horas diárias.
- 2.7.2 O treinamento deverá iniciar em até 5 (cinco) dias úteis após a instalação dos equipamentos, componentes e softwares da solução;

- 2.7.3 O treinamento será de natureza teórica e prática, devendo abranger todos os equipamentos, componentes e softwares das soluções ofertadas, em seus aspectos mais relevantes;
- 2.7.4 A CONTRATADA deverá fornecer material didático individual que abranja todo o conteúdo do curso;
- 2.7.5 O material didático a ser fornecido aos alunos deverá ser previamente aprovado pela CONTRATANTE por meio de amostra que deverá ser entregue, no mínimo, três dias antes do início do curso;
- 2.7.6 A CONTRATADA deverá fornecer certificado individual de conclusão com aproveitamento do curso em até 3 dias úteis após o encerramento do treinamento;
- 2.7.7 Os instrutores deverão ser comprovadamente certificados nos programas e equipamentos fornecidos no escopo da solução;
- 2.7.8 O treinamento deverá ocorrer em período e horário definido pela CONTRATANTE, respeitando as especificações contidas neste item;
- 2.7.9 A qualidade do curso deverá ser avaliada por seus participantes ao final do mesmo e, caso seja considerada insuficiente, a CONTRATADA deverá providenciar a realização de nova turma, até o alcance dos objetivos do treinamento, sem ônus adicional para a Presidência da República;
- 2.7.10 O conteúdo programático do treinamento será definido previamente pela CONTRATANTE em conjunto com a CONTRATADA e deverá abordar, no mínimo, os principais aspectos relativos à solução adquirida e de sua implantação no caso específico da Presidência da República;
- 2.7.11 Para a consecução da parte prática do treinamento deverão ser utilizados equipamentos similares aos ofertados, além de todos os softwares que fizerem parte da solução